	Type	Hits	Search Text	DBs	Time Stamp
1	BRS	724	380/277.ccls.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 09:11
2	BRS	323	713/171.ccls.	USPAT; US-PGPUB; IBM_TDB	2004/09/14 15:14
3	BRS	133	380/260.ccls.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 08:24
4	BRS	193	380/281.ccls.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 09:35
5	BRS	1	5517667.pn.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 09:37
6	BRS	2	(DAQ and electronic$1).as.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 10:40
7	BRS	20	("4731840" | "4850017" | "4864615" | "4876716" | "4933971" | "4944007" | "5029207" | "5124117" | "5136642" | "5144667" | "5146497" | "5146498" | "5150408" | "5159633" | "5164986" | "5173938" | "5177791" | "5202922" | "5319710" | "5392356").PN.	USPAT	2004/09/15 09:40
8	BRS	39	farrugia.in.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 11:05
9	BRS	6	("5517667" "5686904" "5604801" "4935961" "5357571" "4317957").pn.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 11:06
10	BRS	23	4935961.URPN.	USPAT	2004/09/15 11:07
11	BRS	8	5517567.URPN.	USPAT	2004/09/15 12:03
12	BRS	177	key adj storage adj unit	USPAT; US-PGPUB; IBM_TDB	2004/09/15 14:12
13	BRS	1	(key adj storage adj unit).ti.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 15:31
14	BRS	32	smart$1card same key same exchang$3	USPAT; US-PGPUB; IBM_TDB	2004/09/15 16:05
15	BRS	10	software same (unlock or decrypt) same smart$1card	USPAT; US-PGPUB; IBM_TDB	2004/09/15 16:13
16	BRS	10609	(software or program$1) same (unlock$3 or decrypt$3)	USPAT; US-PGPUB; IBM_TDB	2004/09/15 16:14
17	BRS	30	((software or program$1) same (unlock$3 or decrypt$3)).ti.	USPAT; US-PGPUB; IBM_TDB	2004/09/15 16:14
18	BRS	167	(software same protect$3).ti.	USPAT; US-PGPUB; IBM_TDB	2004/09/16 12:12
19	BRS	81	(software same protect$3).ti. and ($5card$1)	USPAT; US-PGPUB; IBM_TDB	2004/09/16 12:13

US005651066A

United States Patent [19]

Moriyasu et al.

[11] Patent Number: 5,651,066

[45] Date of Patent: Jul. 22, 1997

[54] **CIPHER KEY DISTRIBUTION SYSTEM EFFECTIVELY PREVENTING ILLEGITIMATE USE AND CHARGING OF ENCIPHERED INFORMATION**

[75] Inventors: **Kenji Moriyasu**, Tokyo; **Atsusi Kanai**, Kanagawaken; **Nobuhisa Miyake**; **Atsusi Terauchi**, both of Tokyo; **Hironobu Okuyama**, Saitamaken, all of Japan

[73] Assignee: **Nippon Telegraph and Telephone Corporation**, Tokyo, Japan

[21] Appl. No.: **431,407**

[22] Filed: **Apr. 28, 1995**

[30] **Foreign Application Priority Data**

Apr. 28, 1994 [JP] Japan 6-091857

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/21**; 380/23

[58] **Field of Search** 380/21, 49, 28, 380/23, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,341,426	8/1994	Barney et al.	380/21
5,381,479	1/1995	Gardeck et al.	380/21
5,442,703	8/1995	Kim et al.	380/21
5,491,750	2/1996	Bellare et al.	380/21
5,517,567	5/1996	Epstein	380/21
5,544,245	8/1996	Tsubakiyama	380/21

Primary Examiner—David C. Cain

Attorney, Agent, or Firm—Banner & Witcoff, Ltd.

[57] **ABSTRACT**

A method and a system for cipher key distribution realizing an effective prevention of the illegitimate use and the illegitimate charging. A key request signal containing a first random number generated at each user terminal is transmitted from each user terminal to the key center, so as to indicate the cipher key required at each user terminal to the key center, and a terminal check signal containing a second random number generated at the key center is transmitted from the key center to each user terminal. Then, a terminal response signal containing the second random number and a value based on the first random number obtained according to the first random number generated at each user terminal and the second random number contained in the terminal check signal is transmitted from each user terminal to the key center, and the second random number and the value based on the first random number contained in the terminal response signal are checked at the key center, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal. Then, a key distribution signal containing the cipher key requested by the key request signal is transmitted from the key center to each user terminal, only when the legitimacy of the access from each user terminal is confirmed.

20 Claims, 12 Drawing Sheets

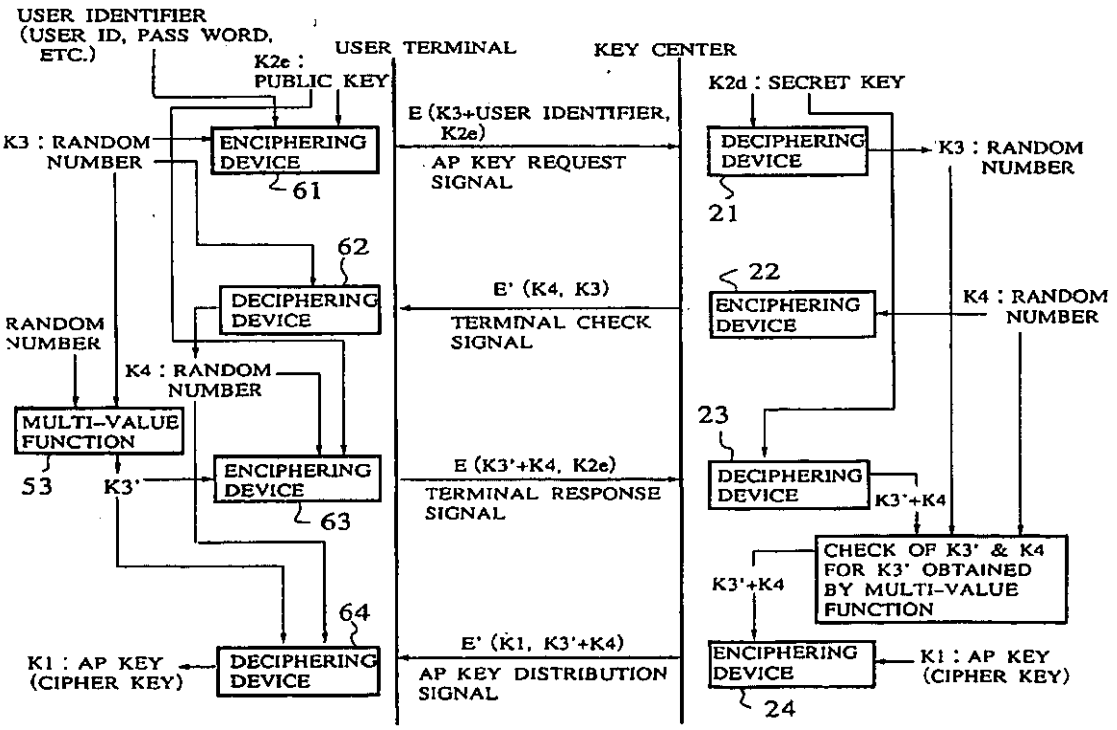


FIG. 1
PRIOR ART

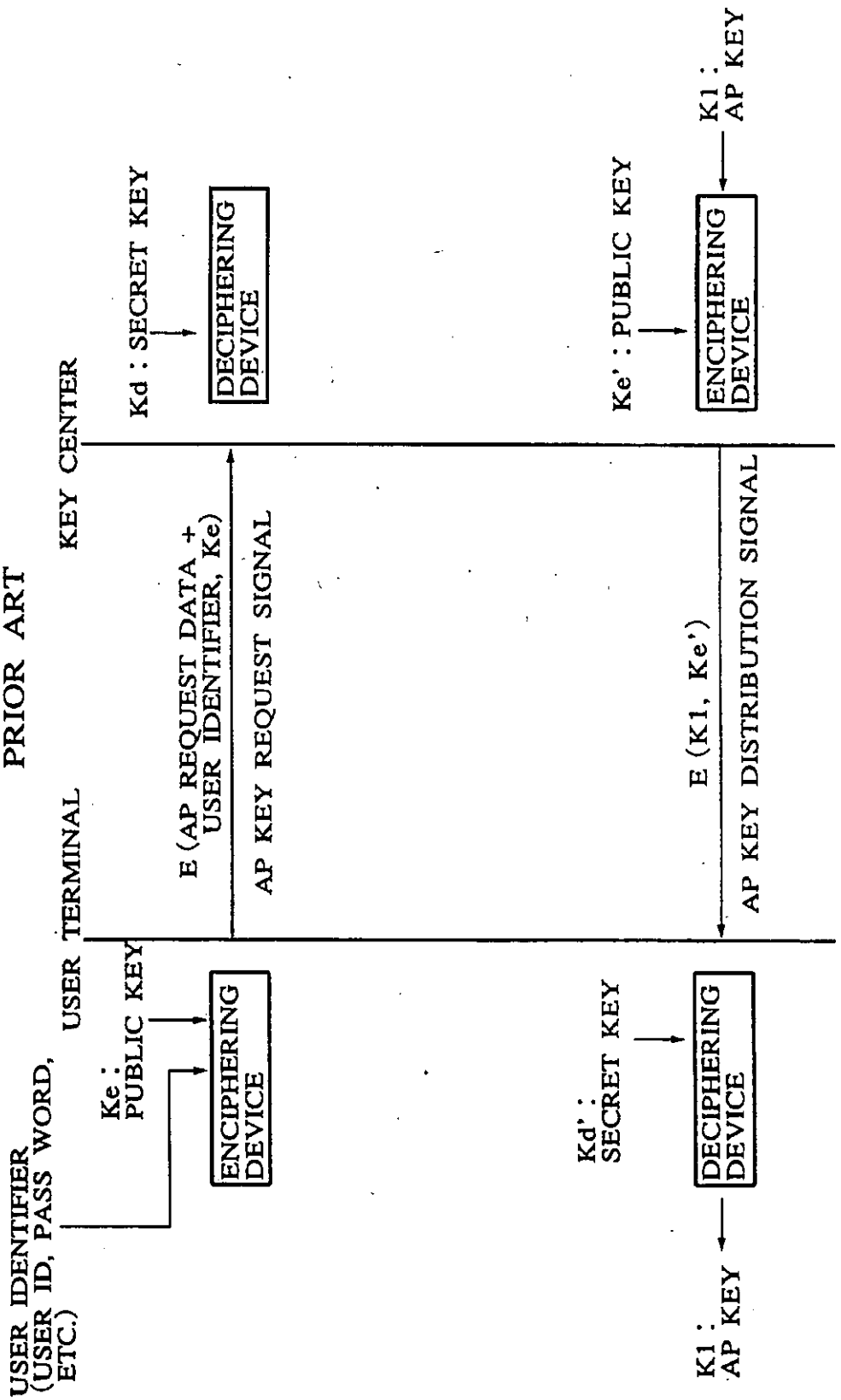


FIG.2
PRIOR ART

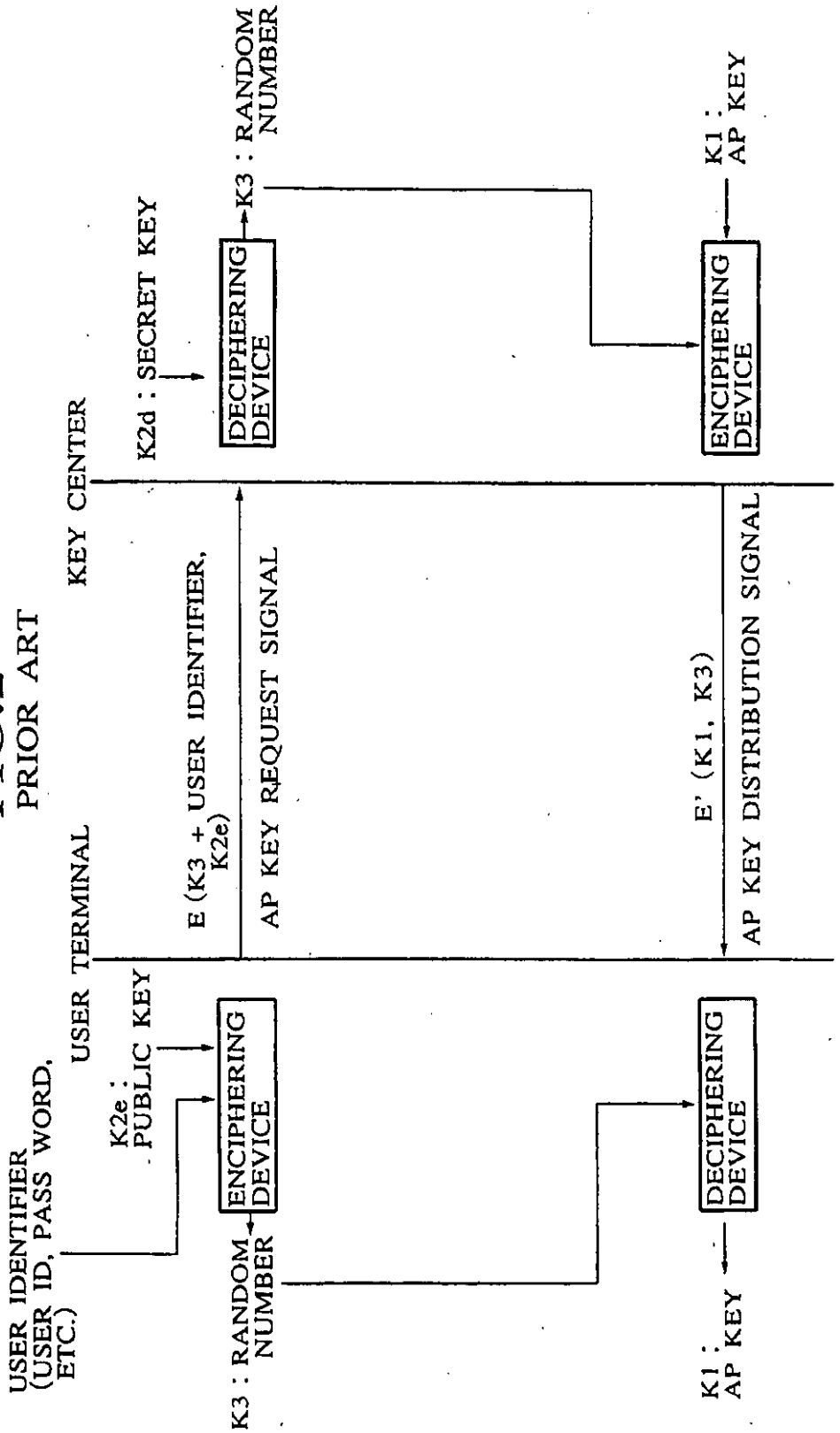


FIG.3

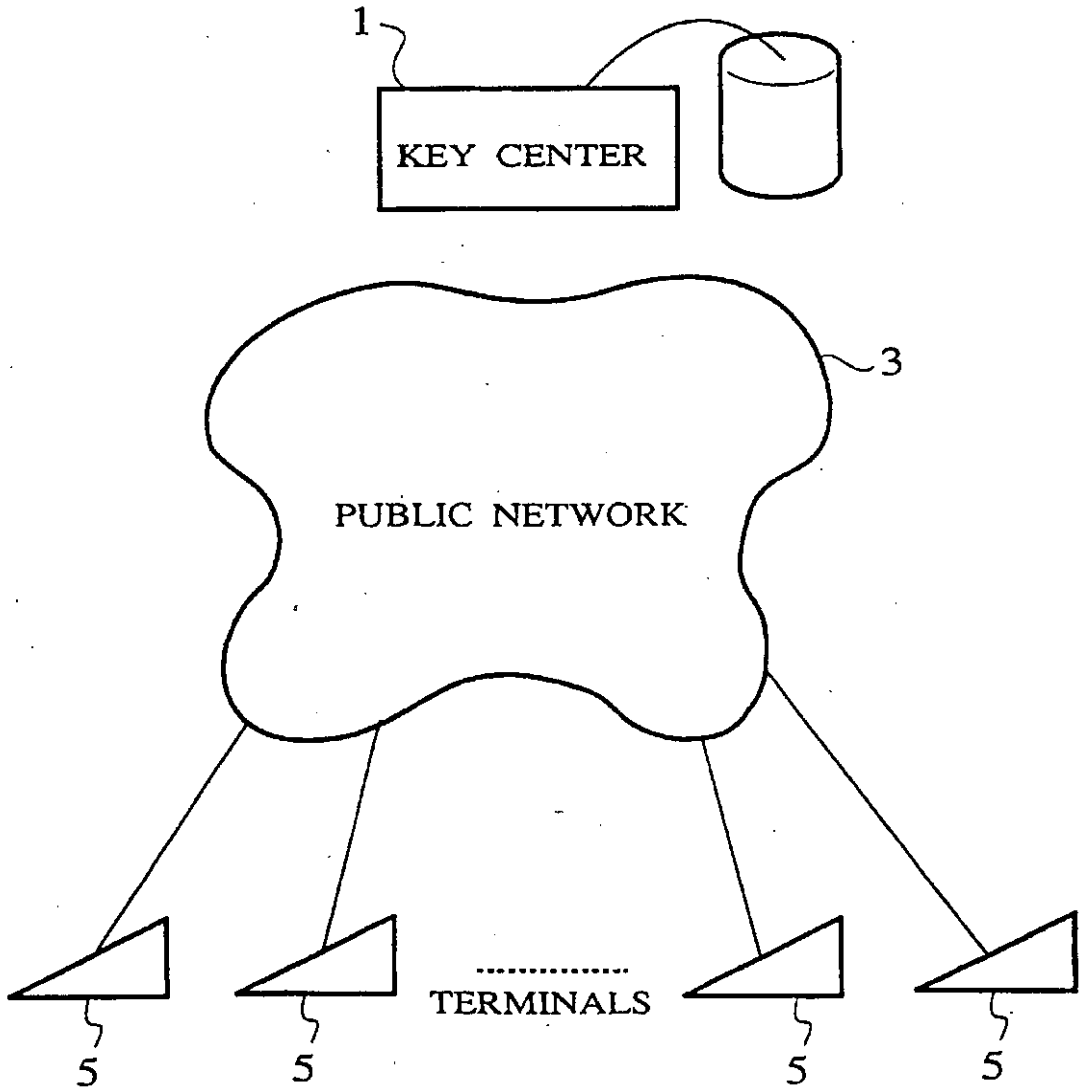


FIG.4

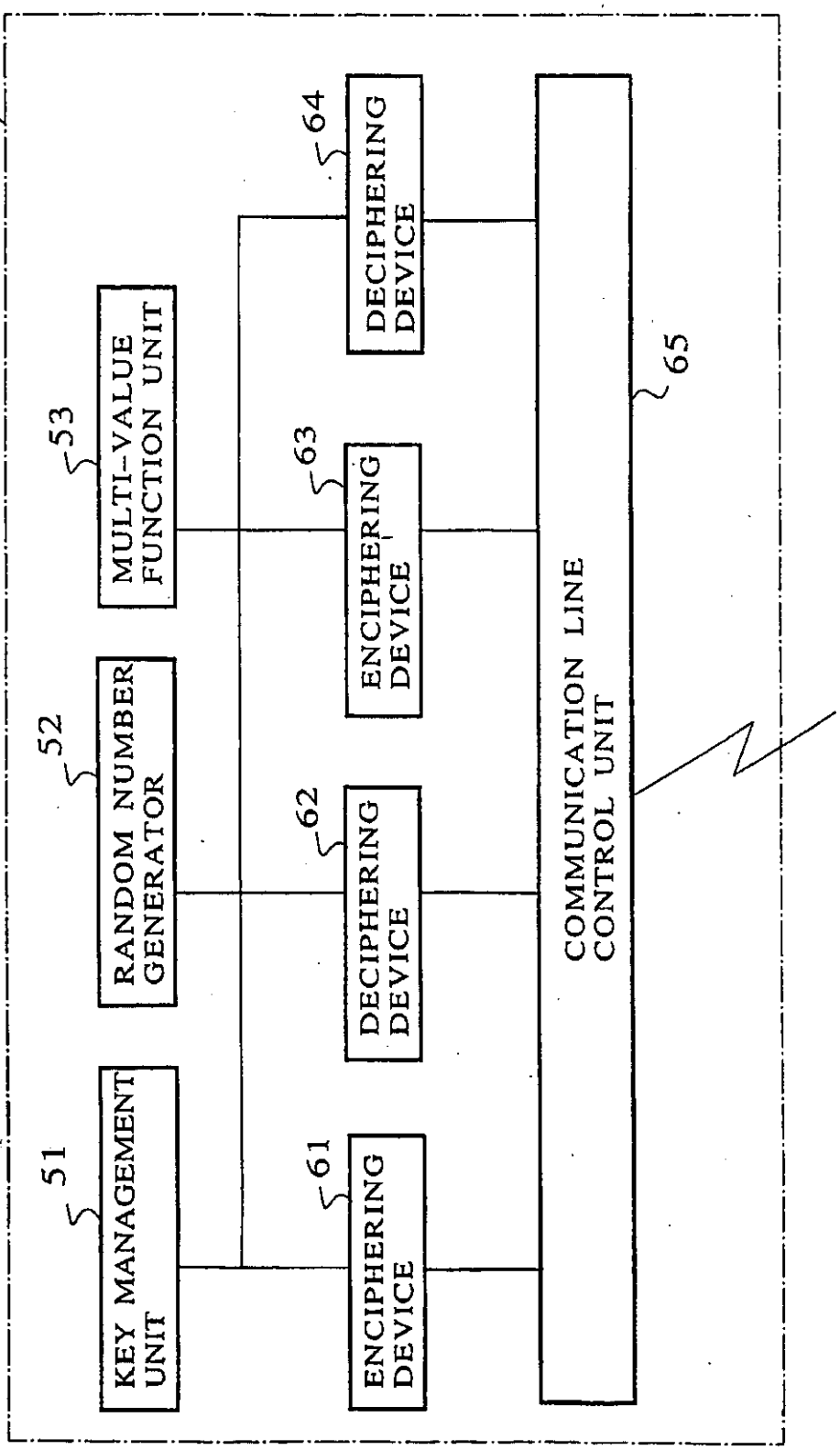

5
KEY MANAGEMENT UNIT
51
RANDOM NUMBER GENERATOR
52
MULTI-VALUE FUNCTION UNIT
53
ENCIPHERING DEVICE
61
DECIPHERING DEVICE
62
ENCIPHERING DEVICE
63
DECIPHERING DEVICE
64
COMMUNICATION LINE CONTROL UNIT
65

FIG.5

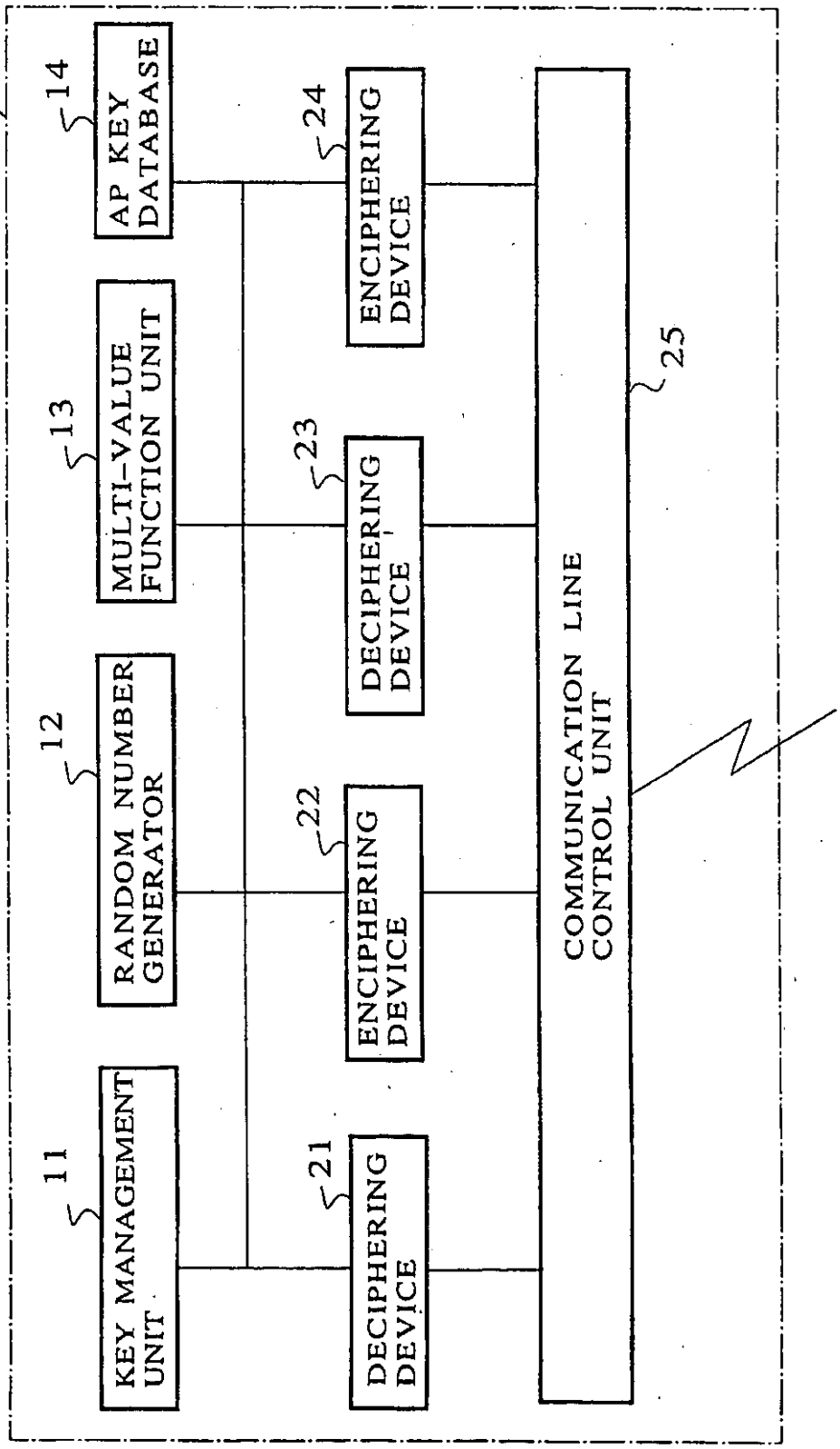

1
11
KEY MANAGEMENT UNIT
12
RANDOM NUMBER GENERATOR
13
MULTI-VALUE FUNCTION UNIT
14
AP KEY DATABASE
21
DECIPHERING DEVICE
22
ENCIPHERING DEVICE
23
DECIPHERING DEVICE
24
ENCIPHERING DEVICE
25
COMMUNICATION LINE CONTROL UNIT

FIG.6

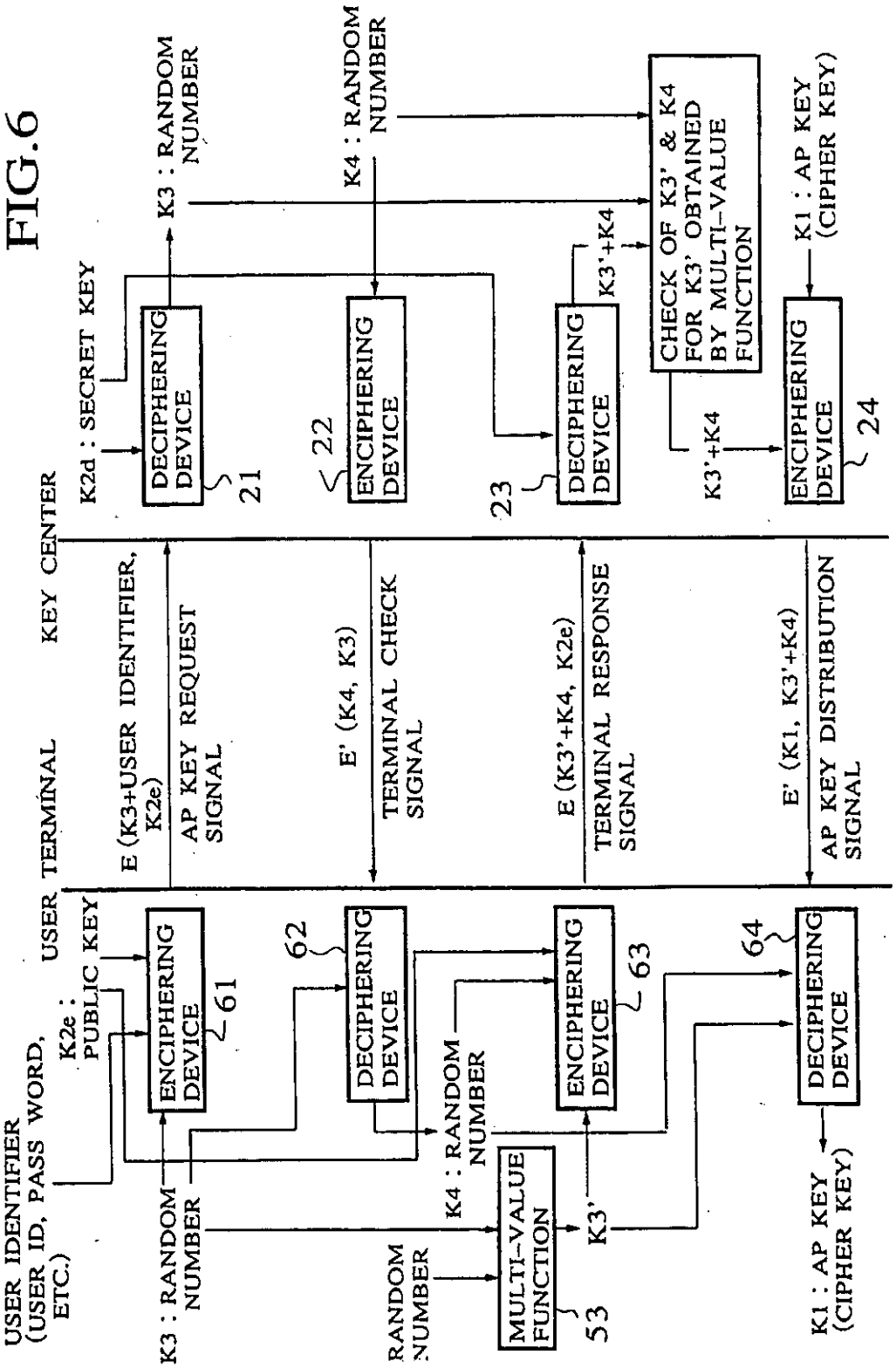

USER IDENTIFIER (USER ID, PASS WORD, ETC.)
K2e : PUBLIC KEY
K3 : RANDOM NUMBER
ENCIPHERING DEVICE
61
DECIPHERING DEVICE
62
RANDOM NUMBER
MULTI-VALUE FUNCTION
53
K4 : RANDOM NUMBER
K3'
ENCIPHERING DEVICE
63
DECIPHERING DEVICE
64
K1 : AP KEY (CIPHER KEY)
USER TERMINAL
KEY CENTER
E (K3+USER IDENTIFIER, K2e)
AP KEY REQUEST SIGNAL
E' (K4, K3)
TERMINAL CHECK SIGNAL
E (K3'+K4, K2e)
TERMINAL RESPONSE SIGNAL
E' (K1, K3'+K4)
AP KEY DISTRIBUTION SIGNAL
K2d : SECRET KEY
DECIPHERING DEVICE
21
K3 : RANDOM NUMBER
22
ENCIPHERING DEVICE
K4 : RANDOM NUMBER
23
DECIPHERING DEVICE
K3'+K4
CHECK OF K3' & K4 FOR K3' OBTAINED BY MULTI-VALUE FUNCTION
K3'+K4
ENCIPHERING DEVICE
24
K1 : AP KEY (CIPHER KEY)

FIG.7

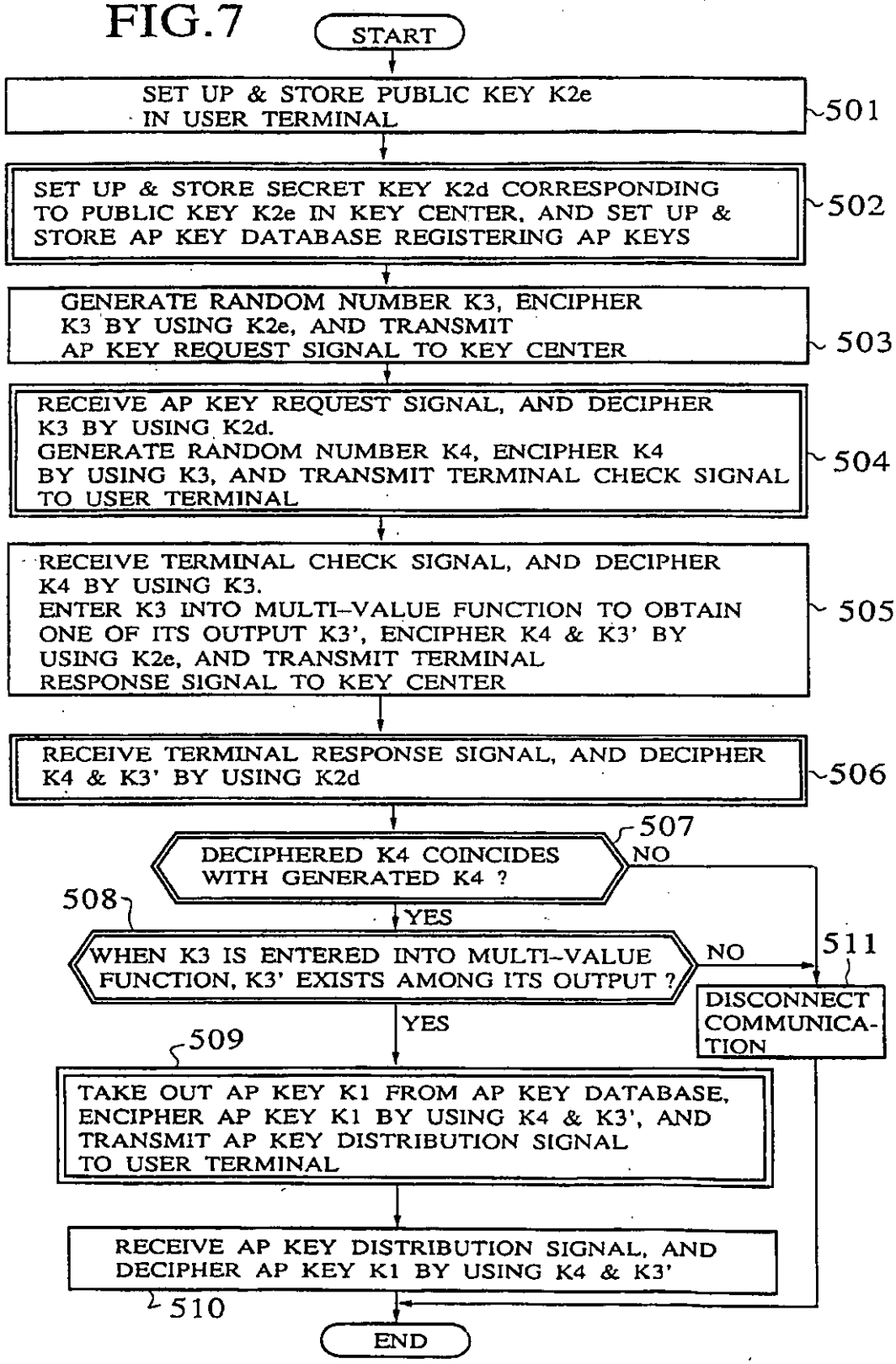

START
SET UP & STORE PUBLIC KEY K2e IN USER TERMINAL
501
SET UP & STORE SECRET KEY K2d CORRESPONDING TO PUBLIC KEY K2e IN KEY CENTER, AND SET UP & STORE AP KEY DATABASE REGISTERING AP KEYS
502
GENERATE RANDOM NUMBER K3, ENCIPHER K3 BY USING K2e, AND TRANSMIT AP KEY REQUEST SIGNAL TO KEY CENTER
503
RECEIVE AP KEY REQUEST SIGNAL, AND DECIPHER K3 BY USING K2d. GENERATE RANDOM NUMBER K4, ENCIPHER K4 BY USING K3, AND TRANSMIT TERMINAL CHECK SIGNAL TO USER TERMINAL
504
RECEIVE TERMINAL CHECK SIGNAL, AND DECIPHER K4 BY USING K3. ENTER K3 INTO MULTI-VALUE FUNCTION TO OBTAIN ONE OF ITS OUTPUT K3', ENCIPHER K4 & K3' BY USING K2e, AND TRANSMIT TERMINAL RESPONSE SIGNAL TO KEY CENTER
505
RECEIVE TERMINAL RESPONSE SIGNAL, AND DECIPHER K4 & K3' BY USING K2d
506
507
DECIPHERED K4 COINCIDES WITH GENERATED K4 ?
NO
YES
508
WHEN K3 IS ENTERED INTO MULTI-VALUE FUNCTION, K3' EXISTS AMONG ITS OUTPUT ?
NO
511
DISCONNECT COMMUNICA-TION
YES
509
TAKE OUT AP KEY K1 FROM AP KEY DATABASE, ENCIPHER AP KEY K1 BY USING K4 & K3', AND TRANSMIT AP KEY DISTRIBUTION SIGNAL TO USER TERMINAL
RECEIVE AP KEY DISTRIBUTION SIGNAL, AND DECIPHER AP KEY K1 BY USING K4 & K3'
510
END

FIG.8

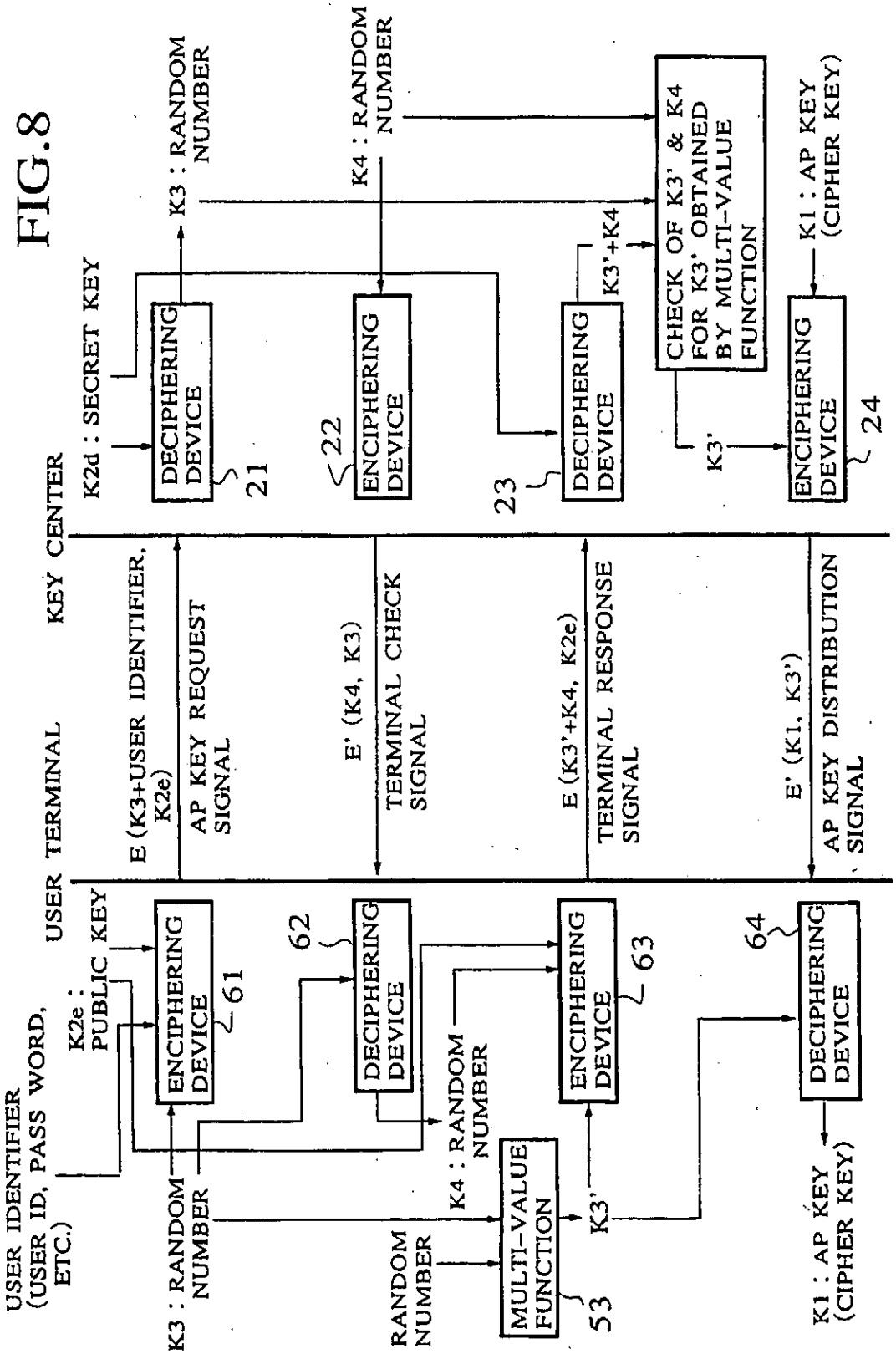

USER IDENTIFIER (USER ID, PASS WORD, ETC.)
K2e : PUBLIC KEY
K3 : RANDOM NUMBER
RANDOM NUMBER
K4 : RANDOM NUMBER
K3'
K1 : AP KEY (CIPHER KEY)
ENCIPHERING DEVICE 61
DECIPHERING DEVICE 62
MULTI-VALUE FUNCTION 53
ENCIPHERING DEVICE 63
DECIPHERING DEVICE 64
USER TERMINAL
KEY CENTER
E (K3+USER IDENTIFIER, K2e)
AP KEY REQUEST SIGNAL
E' (K4, K3)
TERMINAL CHECK SIGNAL
E (K3'+K4, K2e)
TERMINAL RESPONSE SIGNAL
E' (K1, K3')
AP KEY DISTRIBUTION SIGNAL
K2d : SECRET KEY
DECIPHERING DEVICE 21
K3 : RANDOM NUMBER
ENCIPHERING DEVICE 22
K4 : RANDOM NUMBER
DECIPHERING DEVICE 23
K3'+K4
CHECK OF K3' & K4 FOR K3' OBTAINED BY MULTI-VALUE FUNCTION
K3'
ENCIPHERING DEVICE 24
K1 : AP KEY (CIPHER KEY)

FIG.9

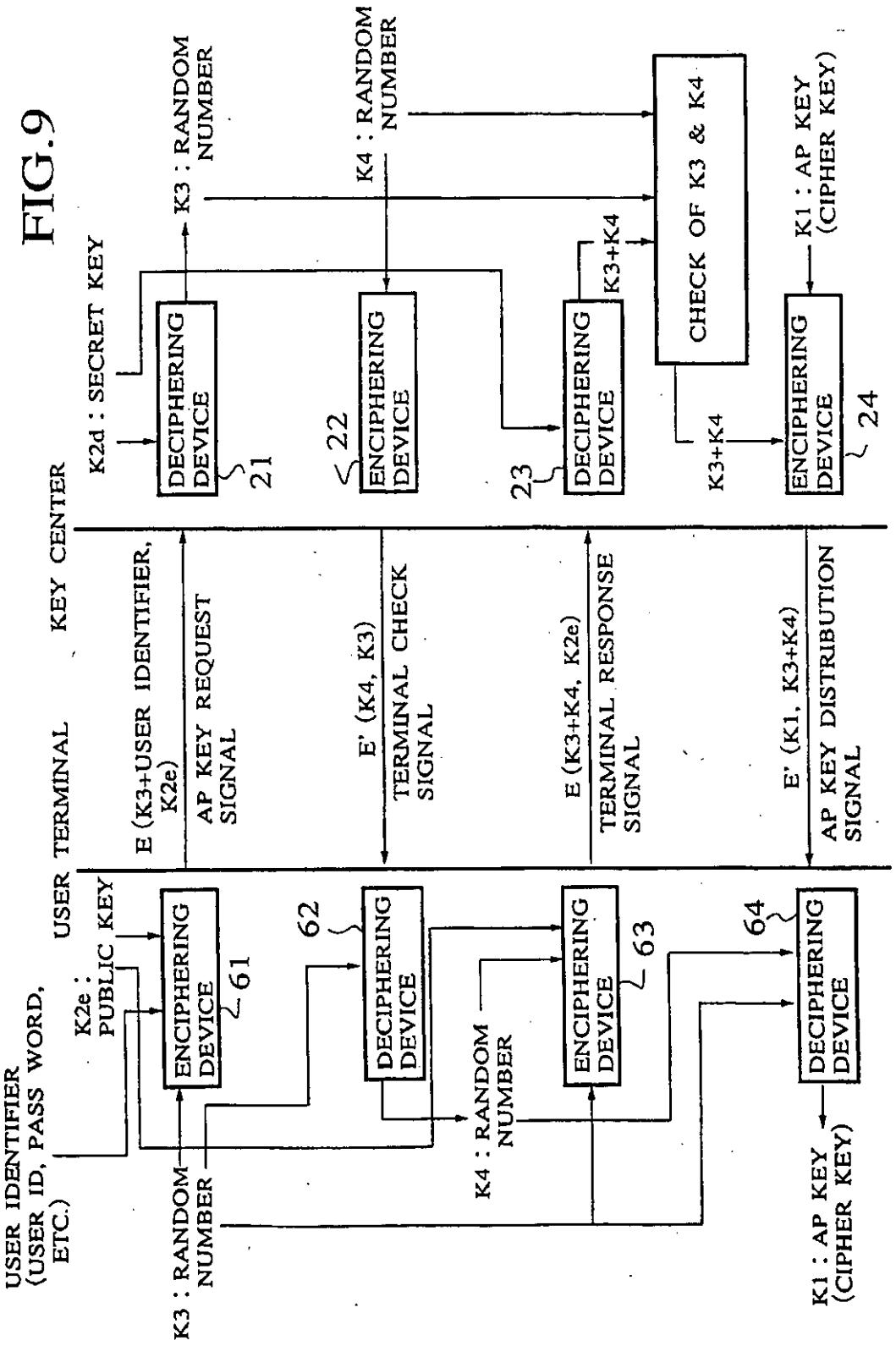

USER IDENTIFIER (USER ID, PASS WORD, ETC.)
K2e : PUBLIC KEY
USER TERMINAL
KEY CENTER
ENCIPHERING DEVICE
61
E (K3+USER IDENTIFIER, K2e)
AP KEY REQUEST SIGNAL
K3 : RANDOM NUMBER
K2d : SECRET KEY
DECIPHERING DEVICE
21
62
DECIPHERING DEVICE
E' (K4, K3)
TERMINAL CHECK SIGNAL
K4 : RANDOM NUMBER
22
ENCIPHERING DEVICE
63
ENCIPHERING DEVICE
E (K3+K4, K2e)
TERMINAL RESPONSE SIGNAL
23
DECIPHERING DEVICE
K3+K4
CHECK OF K3 & K4
64
DECIPHERING DEVICE
E' (K1, K3+K4)
AP KEY DISTRIBUTION SIGNAL
K1 : AP KEY (CIPHER KEY)
K3+K4
ENCIPHERING DEVICE
24
K1 : AP KEY (CIPHER KEY)

FIG.10

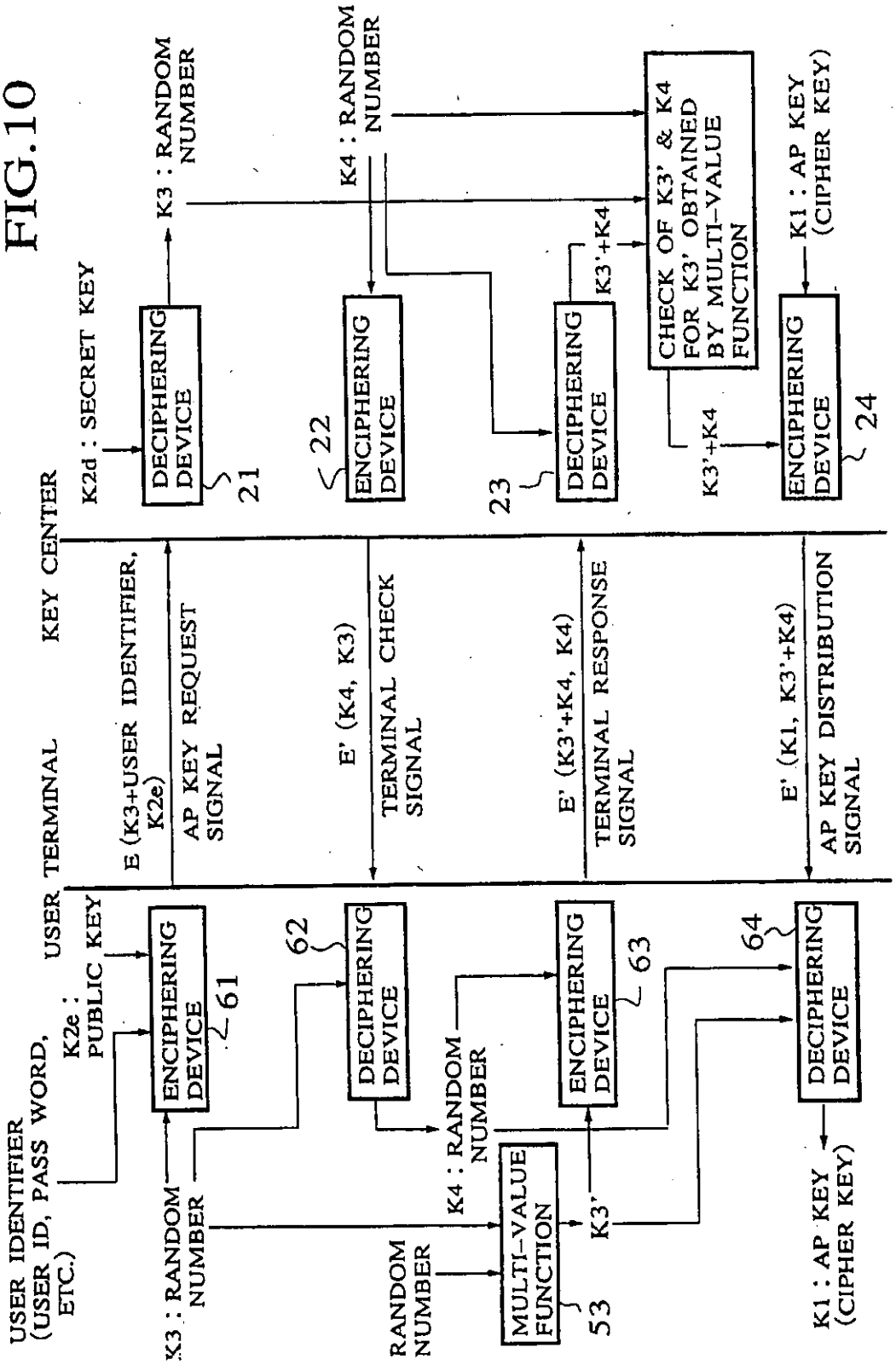

USER IDENTIFIER (USER ID, PASS WORD, ETC.)
K2e : PUBLIC KEY
K3 : RANDOM NUMBER
ENCIPHERING DEVICE
61
DECIPHERING DEVICE
62
USER TERMINAL
KEY CENTER
E (K3+USER IDENTIFIER, K2e)
AP KEY REQUEST SIGNAL
K2d : SECRET KEY
DECIPHERING DEVICE
21
K3 : RANDOM NUMBER
E' (K4, K3)
TERMINAL CHECK SIGNAL
ENCIPHERING DEVICE
22
K4 : RANDOM NUMBER
RANDOM NUMBER
MULTI-VALUE FUNCTION
53
K4 : RANDOM NUMBER
K3'
ENCIPHERING DEVICE
63
E' (K3'+K4, K4)
TERMINAL RESPONSE SIGNAL
DECIPHERING DEVICE
23
K3'+K4
CHECK OF K3' & K4 FOR K3' OBTAINED BY MULTI-VALUE FUNCTION
K3'+K4
ENCIPHERING DEVICE
24
E' (K1, K3'+K4)
AP KEY DISTRIBUTION SIGNAL
DECIPHERING DEVICE
64
K1 : AP KEY (CIPHER KEY)
K1 : AP KEY (CIPHER KEY)

FIG. 11

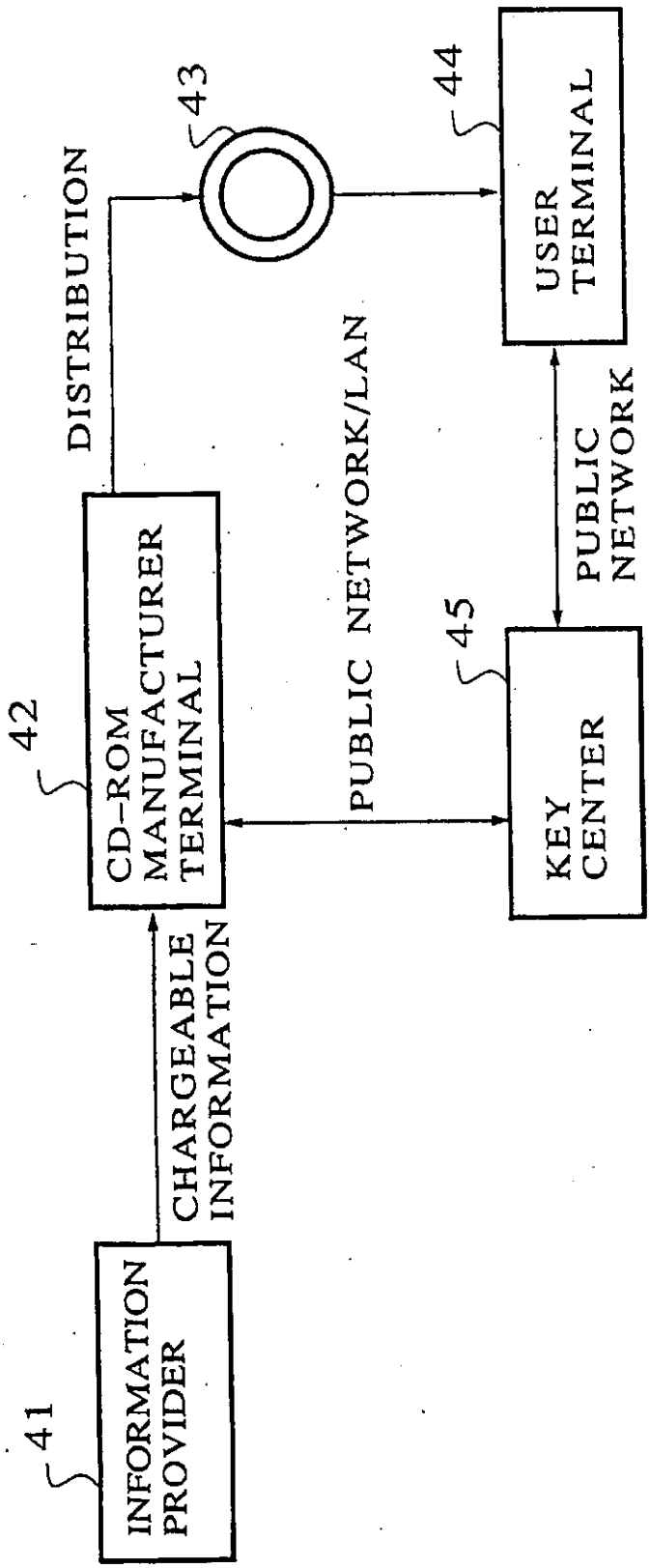
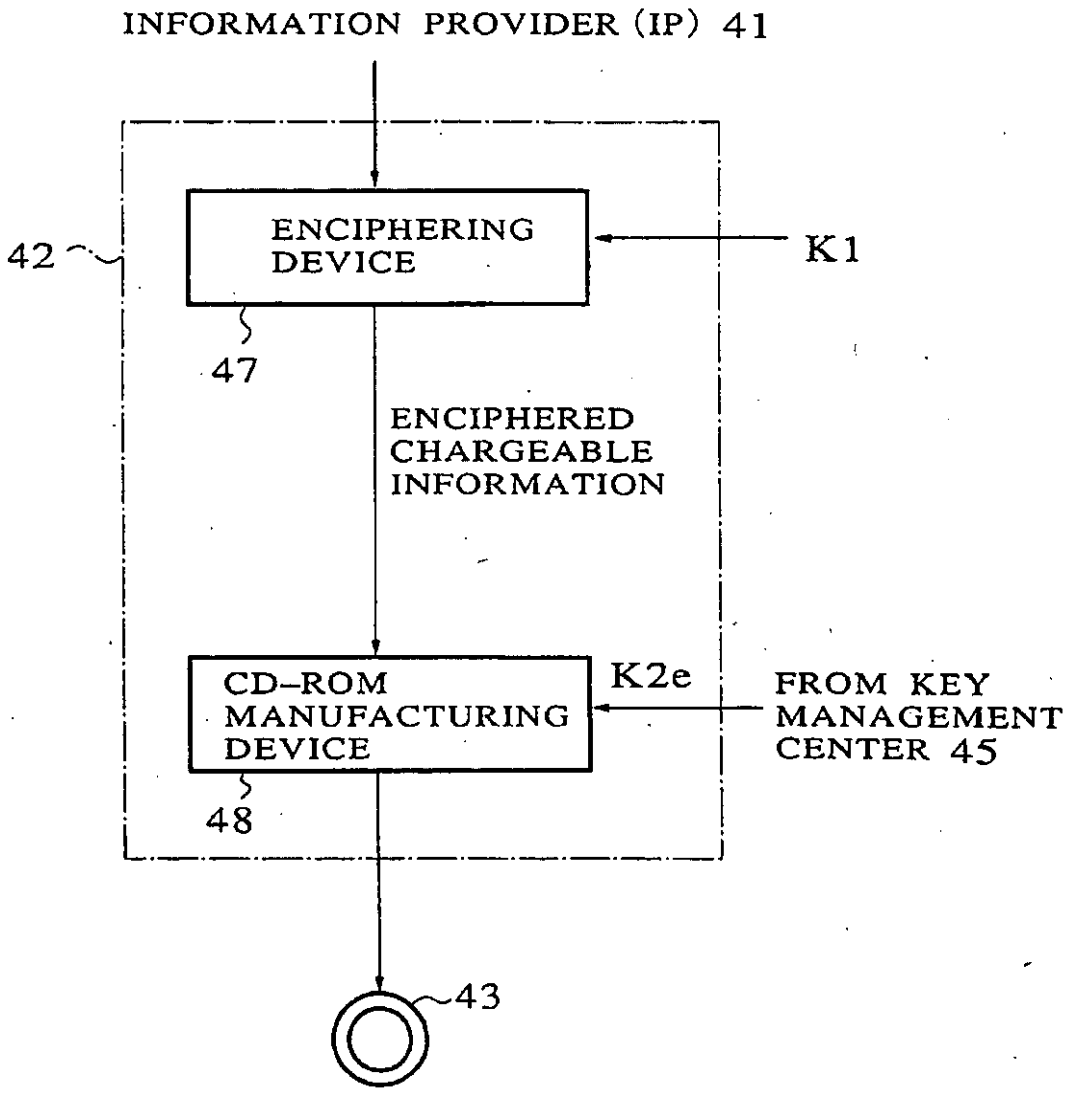

41
INFORMATION PROVIDER
CHARGEABLE INFORMATION
42
CD-ROM MANUFACTURER TERMINAL
DISTRIBUTION
43
44
USER TERMINAL
PUBLIC NETWORK/LAN
PUBLIC NETWORK
45
KEY CENTER

FIG.12


INFORMATION PROVIDER (IP) 41
42
ENCIPHERING DEVICE
K1
47
ENCIPHERED CHARGEABLE INFORMATION
CD-ROM MANUFACTURING DEVICE
K2e
FROM KEY MANAGEMENT CENTER 45
48
43

CIPHER KEY DISTRIBUTION SYSTEM EFFECTIVELY PREVENTING ILLEGITIMATE USE AND CHARGING OF ENCIPHERED INFORMATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a cipher key distribution system for distributing a cipher key from a key center to an unspecified number of user terminals through a public network.

2. Description of the Background Art

In a system formed by a key center and an unspecified number of user terminals connected with the key center through a public network, an enciphered application (AP) and a terminal program necessary for utilizing this system are initially distributed to an unspecified number of user terminals either through the network or by the use of information recording media. In such a system, in order to decipher the AP, the key center distributes a certain cipher key (referred hereafter as an AP key) to the user terminals.

Now, such a system ideally should satisfy the following conditions.

(1) A terminal program cannot be analyzed at the user terminal.

(2) An AP key obtained at the user terminal and a program for deciphering the AP are protected against an illegitimate use.

(3) A cipher scheme of the enciphered AP which is distributed to the terminal users and a cipher scheme for enciphering signals on communication lines have sufficient secrecy.

In the following, a use of the AP by a terminal user without using a connection with the key center through a legitimate protocol will be referred as an illegitimate use.

In general, for the condition (3), there are some propositions for a scheme which can guarantee a certain level of secrecy. However, for the conditions (1) and (2), there are cases in which it may be difficult to adopt a scheme relying on a specialized hardware for reasons such as that of cost, etc., and there is a need to provide a software based protection scheme. In such a software based protection scheme, however, a level of protection is a matter of relative significance because the analysis of the terminal program is still possible in principle, and the acquisition of the AP key obtained at the user terminal is also still possible.

In the above described system, depending on a protocol scheme used between the user terminal and the key center, the illegitimate use by a malicious terminal user is possible by means of the tapping of signal on the communication line between the key center and the user terminal.

For example, consider a conventional protocol scheme as shown in FIG. 1 in which the AP key is simply enciphered and distributed from the key center in response to the request for the AP key from the user terminal. This scheme will be referred hereafter as a conventional scheme A.

In this conventional scheme A, at the user terminal, the AP key request signal is produced by enciphering a user identifier such as user ID, pass word, etc., and an AP request data necessary for requesting a desired AP in a public key enciphering scheme E using a public key Ke that was distributed in advance as a cipher key, and transmitted to the key center. Then, at the key center, the received AP key request signal is deciphered by using a secret key Kd

corresponding to the public key Ke, and an AP key distribution signal is produced by enciphering a decipher key (AP key) K1 of the requested AP in the public key enciphering scheme using a public key Ke' as a cipher key, and transmitted to the user terminal, while charging the fee for the requested AP to the user. Then, at the user terminal, the AP key distribution signal is deciphered by using a secret key Kd' corresponding to the public key Ke' that was distributed in advance, to obtain the AP key K1 of the desired AP. In this procedure, the transmission of the user identifier from the user terminal to the key center may be omitted.

Here, it is noted that the secret key enciphering scheme is a scheme in which the cipher key and the decipher key are the same, whereas the public key enciphering scheme is a scheme in which the cipher key and the decipher key are different. In the conventional scheme A described above, the public key enciphering scheme is used, but if the key can be shared secretly and safely in some manner at the beginning, it is also possible to consider a case of using the secret key enciphering scheme instead of the public key enciphering scheme.

In this conventional scheme A, even when the system satisfies all the conditions (1) to (3) noted above, it is still possible to make the illegitimate use of the AP as follows. Namely, the key center transmits the same AP key for the same AP, so that the same AP key distribution signal is going to be transmitted through the communication line every time the same AP is requested. Consequently, the illegitimate use is possible by recording the AP key distribution signal at a time of connecting with the key center once, and forming a dummy key center which reproduces the recorded AP key distribution signal. In other words, this is an illegitimate use of the AP by a fake key center using communication line tapping and recording.

This type of the illegitimate use is effective in a case of using the charging method in which each time of the use of the AP is charged separately. In such a case, the user terminal is going to receive the same AP key distribution signal for every time of the use of the same AP, so that it is possible to make the legitimate use in the first occasion in order to tap and record the AP key distribution signal, and input the recorded signal into the user terminal without connecting with the key center in the subsequent occasions.

Note however that, in this type of the illegitimate use, it is necessary to make the legitimate connection with the key center in the first occasion at least. For this reason, in a case of using the charging method in which the AP software itself is sold once and for all, this type of the illegitimate use is impossible, because in such a case, the same AP key will never be received again once the key for the AP is received from the key center at the user terminal.

On the other hand, in order to deal with this type of the illegitimate use, consider another conventional protocol scheme as shown in FIG. 2 in which the user terminal generates a random number and transmits that to the key center, and the key center enciphers and distributes the AP key according to the received random number. This scheme will be referred hereafter as a conventional scheme B.

In this conventional scheme B, at the user terminal, the AP key request signal is produced by enciphering a user identifier such as a user ID, pass word, etc., an AP request data necessary for requesting a desired AP, and a random number K3 generated at the terminal in a public key enciphering scheme E using a public key K2*e* that was distributed in advance as a cipher key, and transmitted to the key center. Then, at the key center, the received AP key request signal

is deciphered by using a secret key K2*d* corresponding to the public key K2*e*, and an AP key distribution signal is produced by enciphering a decipher key (AP key) K1 of the requested AP in the secret key enciphering scheme E' using the random number K3 as a cipher key, and transmitted to the user terminal. Then, at the user terminal, the AP key distribution signal is deciphered by using the random number K3 generated earlier, to obtain the AP key K1 of the desired AP. In this procedure, the transmission of the user identifier from the user terminal to the key center may be omitted.

According to this conventional scheme B, a different signal flows through a communication line each time, so that, when the system satisfies the conditions (1) to (3) noted above, even if a third person intending the illegitimate use of the AP produces a dummy key center by tapping and recording the signal on the communication line and inputs the recorded signal into own terminal program, whether the inputted signal is enciphered by the same random number as that which was generated earlier at that user terminal or not is checked inside the user terminal, so that it is impossible to make the above described illegitimate use of the AP.

However, in this conventional scheme B, even when the conditions (1) to (3) noted above are satisfied, it is still possible to make the following illegitimate action which is different from the above described illegitimate use of the AP.

Namely, the third person can tap and record the signal from a legitimate user terminal to the key center, and then transmits the recorded signal to the key center later on. Here, if the public network used in this service is a type which does not have a function for confirming a calling side ID as in a case of the telephone network, it is possible to reproduce an information transmitted from the user terminal to the key center for the purpose of authenticating the calling side, by tapping and recording of the signal on the communication line in principle. When the AP key request signal from the user terminal is received, the key center transmits the AP key distribution signal corresponding to that, and charges the fee for the requested AP to the user when the requested AP is a chargeable one.

In this manner, the third person can makes the key center to transmit an unnecessary AP key to the legitimate user, and charge unnecessary fees to the legitimate user. In other words, this is an illegitimate charging by a fake user terminal using communication line tapping and recording.

Moreover, as already mentioned above, the conditions (1) and (2) noted above may not necessarily be satisfied completely all the times. In particular, in a case of using a protection based on the software technique, the analysis of the terminal software is often possible in principle albeit not so easy.

In such a case, the tapping and the recording of the signals on the communication line is the easiest thing one can do toward the program analysis. This is because when the meaning of the input output signals of the terminal program are analyzed, it is possible to reveal the function of the terminal program itself.

For example, for the conventional scheme B described above, the following procedure is predictable. First, the legitimate use of the AP is made, and the analysis of the meaning is carried out. The enciphered AP is disposed at hand of the terminal user from the beginning and it does not change in time, so that the AP key for deciphering the same AP also does not change in time. On the other hand, by means of the tapping of the communication line, it can be recognized that the received signal of the terminal program is different for the same AP each time, so that it can be recognized that the received signal is changed in some manner such as that which uses a random number.

Here, however, in order for the user terminal side to obtain the AP key by deciphering the received signal, it is necessary to learn a rule by which this constantly changing received signal is changing. In this regard, in the conventional scheme B, the signals are exchanged only once, so that it is evident that the user terminal side is specifying this rule for change at first. Consequently, by checking the rule for change specified by the terminal program, it is possible to obtain an information useful for the purpose of the illegitimate use.

In the conventional scheme B, when the terminal program is analyzed from such a viewpoint, even if the content of the signal itself cannot be revealed as it is enciphered, the meaning of each signal can be determined almost uniquely by conjecturing from the fact that the AP key itself does not change and the fact that the signals actually transmitted and received change. Thus, except for a case in which the analysis is impossible in principle, the difficulty in the analysis can be reduced considerably in this manner.

As described, a mere encipherment of the information on the communication line, and a simple variation of the signal on the communication line based on a random number are insufficient in coping with the problems of the illegitimate use and the illegitimate charging described above.

Furthermore, in a case of realizing a protection of the terminal program by means of software alone, without any hardware based protection, the analysis can be made difficult at best, and it remains possible in principle in many cases.

The user intending the illegitimate use of the AP can carry out the tapping and the recording of the signals on the communication line by using his own user terminal, for the purpose of analyzing the terminal program. In this case, by tapping and recording the signals between the user terminal and the key center for several times and simply comparing these recorded signals, an information useful for the purpose of analyzing the terminal program can be obtained.

Thus, in a situation in which the terminal program analysis or the illegitimate action using intermediate communication line tapping and recording by a malicious terminal user is possible, a mere encipherment of the signal on the communication line or a complication of the terminal program itself is insufficient as the protection against the illegitimate use, and it is necessary to deal with the problems of the illegitimate use and the illegitimate charging based on the production of the dummy key center or user terminal and the simplification of the analysis of the terminal program.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a cipher key distribution system capable of realizing a safe cipher key distribution and an effective prevention of the illegitimate use and the illegitimate charging, by preventing the production of the dummy key center or user terminal while providing little hints for the analysis of the terminal program.

According to one aspect of the present invention there is provided a method of cipher key distribution in a system formed by a key center having a cipher key to be distributed and a plurality of user terminals connected with the key center through a public network, the method comprising the steps of: (a) transmitting a key request signal containing a first random number generated at each user terminal, from each user terminal to the key center, so as to indicate the

cipher key required at each user terminal to the key center; (b) transmitting a terminal check signal containing a second random number generated at the key center, from the key center to each user terminal; (c) transmitting a terminal response signal containing the second random number and a value based on the first random number obtained according to the first random number generated at each user terminal and the second random number contained in the terminal check signal, from each user terminal to the key center; (d) checking the second random number and the value based on the first random number contained in the terminal response signal at the key center, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and (e) transmitting a key distribution signal containing the cipher key requested by the key request signal, from the key center to each user terminal, only when the legitimacy of the access from each user terminal is confirmed at the step (d).

According to another aspect of the present invention there is provided a cipher key distribution system, comprising: a key center having a cipher key to be distributed; a plurality of user terminals connected with the key center through a public network; key request means, provided in each user terminal, for transmitting a key request signal containing a first random number generated at each user terminal, from each user terminal to the key center, so as to indicate the cipher key required at each user terminal to the key center; terminal check means, provided in the key center, for transmitting a terminal check signal containing a second random number generated at the key center, from the key center to each user terminal; terminal response means, provided in each user terminal, for transmitting a terminal response signal containing the second random number and a value based on the first random number obtained according to the first random number generated at each user terminal and the second random number contained in the terminal check signal, from each user terminal to the key center; check means, provided in the key center, for checking the second random number and the value based on the first random number contained in the terminal response signal, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and key distribution means, provided in the key center, for transmitting a key distribution signal containing the cipher key requested by the key request signal, from the key center to each user terminal, only when the legitimacy of the access from each user terminal is confirmed by the check means.

According to another aspect of the present invention there is provided a cipher key distribution system, comprising: a key center having a cipher key to be distributed; and a plurality of user terminals connected with the key center through a public network; wherein each user terminal includes: means for transmitting a key request signal to the key center, receiving a terminal check signal from the key center in response to the key request signal, transmitting a terminal response signal to the key center in response to the terminal check signal, and receiving a key distribution signal from the key center in response to the terminal response signal; means for generating a first random number; means for producing the key request signal containing the first random number, for indicating the cipher key required at each user terminal; means for obtaining a second random number from the terminal check signal received from the key center; means for obtaining a value based on the first random number; means for producing the terminal response signal containing the second random number contained in the terminal check signal and the value based on the first random number; and means for obtaining the cipher key from the key distribution signal received from the key center; and wherein the key center includes: means for receiving the key request signal from each user terminal, transmitting the terminal check signal to each user terminal in response to the key request signal, receiving the terminal response signal from each user terminal in response to the terminal check signal, and transmitting the key distribution signal to each user terminal in response to the terminal response signal; means for obtaining the first random number from the key request signal received from each user terminal; means for generating the second random number; means for producing the terminal check signal containing the second random number; means for obtaining the value based on the first random number and the second random number from the terminal response signal received from each user terminal; means for checking the second random number and the value based on the first random number contained in the terminal response signal, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and means for producing the key distribution signal containing the cipher key requested by the key request signal, only when the legitimacy of the access from each user terminal is confirmed by said means for checking.

Other features and advantages of the present invention will become apparent from the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a chart showing a flow of processing between a user terminal and a key center in one example of a conventional cipher key distribution scheme.

FIG. 2 is a chart showing a flow of processing between a user terminal and a key center in another example of a conventional cipher key distribution scheme.

FIG. 3 is a schematic block diagram showing an overall configuration of one embodiment of a cipher key distribution system according to the present invention.

FIG. 4 is a block diagram of a user terminal in the cipher key distribution system of FIG. 3.

FIG. 5 is a block diagram of a key center in the cipher key distribution system of FIG. 3.

FIG. 6 is a chart showing a flow of processing between a user terminal and a key center in the cipher key distribution system of FIG. 3.

FIG. 7 is a flow chart of the operation at a user terminal and a key center in the cipher key distribution system of FIG. 3.

FIG. 8 is a chart showing a flow of processing to be carried out between a user terminal and a key center in one modification of the cipher key distribution system of FIG. 3.

FIG. 9 is a chart showing a flow of processing to be carried out between a user terminal and a key center in another modification of the cipher key distribution system of FIG. 3.

FIG. 10 is a chart showing a flow of processing to be carried out between a user terminal and a key center in another modification of the cipher key distribution system of FIG. 3.

FIG. 11 is a schematic block diagram of a software sales system utilizing the cipher key distribution method according to the present invention.

FIG. 12 is a block diagram of a CD-ROM manufacturer terminal in the software sales system of FIG. 10.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Now, one embodiment of the cipher key distribution system according to the present invention will be described in detail.

In this embodiment, the cipher key distribution system has an overall configuration as shown in FIG. 3, which comprises a key center 1 having a cipher key (referred hereafter as AP key) to be distributed, and a plurality of user terminals 5 connected with the key center 1 through a public network 3. In this system of FIG. 3, when the AP key becomes necessary at the user terminal 5, the user terminal 5 is connected with the key center 1 through the public network 3 so as to receive the distribution of the AP key from the key center 1.

Each user terminal 5 has a configuration as shown in FIG. 4, which comprises a key management unit 51, a random number generator 52, a multi-value function unit 53, an enciphering device 61, a deciphering device 62, and an enciphering device 63, a deciphering device 64, all of which are mutually connected, and a communication line control unit 65 which is connected with the enciphering and deciphering devices 61, 62, 63, and 64 on one hand and with the public network 3 on the other hand. Functions of these elements of the user terminal 5 will be described in detail below.

Also, the key center 1 has a configuration as shown in FIG. 5, which comprises a key management unit 11, a random number generator 12, a multi-value function unit 13, an AP key database 14, a deciphering device 21, an enciphering device 22, a deciphering device 23, and an enciphering device 24, which are mutually connected, and a communication line control unit 25 which is connected with the deciphering and enciphering devices 21, 22, 23, and 24 on one hand and with the public network 3 on the other hand. Functions of these elements of the user terminal 5 will be described in detail below.

FIG. 6 shows a flow of processing among the user terminal 5 and the key center 1 in this embodiment. In FIG. 6, a symbol E(X, Y) indicates a signal in which X is enciphered in the public key enciphering scheme E using a key Y, and a symbol E'(X, Y) indicates a signal in which X is enciphered in the secret key enciphering scheme E' using a key Y. In this embodiment, it is assumed that the user terminal 5 has a public key K2*e* from the beginning.

Now, the flow of processing shown In FIG. 6 will be described according to the flow chart of FIG. 7. In this flow chart of FIG. 7, steps indicated by double lined boxes belong to the processing at the key center 1, while steps indicated by single lined boxes belong to the processing at the user terminal 5.

First, in the initial state, the user terminal 5 sets up and stores the public key K2*e* in the key management unit 51 (step 501), while the key center 1 sets up and stores the secret key K2*d* corresponding to the public key K2*e* in the key management unit 11 as well as the AP keys to be distributed to the user terminals 5 in the AP key database 14 (step 502).

When the user terminal 5 requires the AP key K1, a random number K3 is generated at the random number generator 52, and a signal E(K3, K2*e*) obtained by enciphering the generated random number K3 by using the public key K2*e* stored in the key management unit 51 at the enciphering device 61 is transmitted as an AP key request signal from the communication line control unit 65 to the key center 1 (step 503).

At this point, if the user identifier such as a user ID, pass word, or both of them, etc. is also required, it is enciphered and transmitted along with the random number K3, but this transmission of the user Identifier may be omitted.

In the key center 1 which received the AF key request signal the random number K3 is deciphered by using the secret key K2*d* stored in the key management unit 11 at the deciphering device 21. Then, a random number K4 is generated at the random number generator 12, and a signal E'(K4, K3) obtained by enciphering the generated random number K4 by using the deciphered random number K3 at the enciphering device 22 is transmitted as a terminal check signal from the communication line control unit 25 to the user terminal 5 (step 504).

Here, which AP key of which AP is requested by the user terminal 5 is indicated in the AP key request signal described above, and the key center 1 can recognize this information from the received AP key request signal.

In the user terminal 5 which received the terminal check signal, the random number K4 is deciphered by using the random number K3 at the deciphering device 62. In addition, this random number K3 is inputted into the multi-value function unit 53, and an arbitrary one of its outputs K3' is obtained. Then, a signal E(K3'+K4, K2*e*) obtained by enciphering the deciphered random number K4 and multi-value function output K3' by using the public key K2*e* at the enciphering device 63 is transmitted as a terminal response signal to the key center 1 (step 505).

In the key center 1 which received the terminal response signal, the random number K4 and the multi-value function output K3' are deciphered by using the secret key K2*d* at the deciphering device 23 (step 506). Then, whether the deciphered random number K4 coincides with that which was generated earlier at the random number generator 12 or not is checked (step 507). If it coincides, the random number K3 is inputted into the multi-value function unit 13 and whether the deciphered multi-value function output K3' exists among a set of outputs produced by the multi-value function unit 13 or not is checked (step 508). If it exists, i.e., when these two conditions of the steps 507 and 508 are satisfied, it is Judged as a legitimate access from a proper user terminal, so that the requested AP key K1 is taken out from the AP key database 14, and a signal E'(K1, K3'+K4) obtained by enciphering this AP key K1 by using the random number K4 and the multi-value function output K3' at the enciphering device 24 is transmitted as an AP key distribution signal to the user terminal 5 8step 509).

On the other hand, when either one of the two conditions of the steps 507 and 508 is not satisfied, it is judged as an illegitimate access from an improper user terminal, so that the communication is disconnected (step 511).

Finally, in the user terminal 5 which received the AP key distribution signal, the AP key K1 is obtained by deciphering the received AP key distribution signal by using the random number K4 and the multi-value function output K3' at the deciphering device 64 (step 510).

Now, the effect of the cipher key distribution system of this embodiment will be described.

As already mentioned above, in a situation in which the illegitimate action using intermediate communication line tapping and recording by a malicious terminal user is possible, a mere encipherment of the signal on the communication line is insufficient as the protection against the

illegitimate use. In view of this fact, the effect of the present invention is to prevent the illegitimate charging by the fake user terminal using the tapping and recording of the signals on the intermediate communication line, as well as a meaning analysis of the signals which can be a powerful and easily obtainable supporting material for the analysis of the terminal program.

In the system which satisfies the conditions (1) to (3) noted above, suppose that a third person intends to make the illegitimate charging to a certain terminal user by means of the fake user terminal using the tapping and recording of the signals on the communication line. Namely, the third person taps and records the signals on the communication line while this terminal user carries out a normal legitimate use of the AP. Then, the third person transmits the output signal of the terminal user side to the key center again later on.

However, according to this embodiment, the signals are exchanged twice for each use of the AP, so that it is necessary for the third person to transmits two signals in an order, but the key center **1** generates a random number each time, so that the random number at a time the signal is recorded by the third person will be different from the random number at a time the illegitimate charging is attempted, and it is possible for the key center **1** to notice that some illegitimate action has been attempted.

Next, in the system which satisfies the condition (3) noted above, but not the conditions (1) and (2) completely, suppose that the terminal user intending to make the meaning analysis of the signals carried out a normal legitimate use of the AP several times, and attempted to tap and record the signals on the communication line to analyze them.

However, according to this embodiment, the signals are exchanged twice, so that it is impossible to know which information is carried by which signal, before analyzing the terminal program itself. Also, as the condition (3) is satisfied, it is also impossible to decipher the signal itself. Consequently, the meaning of the signal cannot be determined uniquely by a simple tapping of the communication line, and therefore the difficulty in the analysis of the terminal program cannot be reduced.

Also, according to this embodiment, the multi-value function output K3' is generated from the random number K3. By means of this, the multi-value function output K3' which is transmitted from the user terminal **5** to the key center **1** as the terminal response signal will not be uniquely determined in total dependence to the random number K3 so that even when the random number K3 is identified in some manner, and the signal E(K4, K3) is identified by the recording, the terminal response signal E(K3'+K4, K2*e*), which is the second output of the terminal program, cannot be identified. On the other hand, the key center **1** has the same multi-value function, so that it is possible to check whether the multi-value function output K3' obtained from the received terminal response signal E(K4+K3', K2*e*) was generated from the random number K3 or not, and therefore it is possible to confirm that the currently communicating terminal program is a proper one originally provided.

Here, the multi-value function is a function which outputs a plurality of fixed values with respect to one input. Thus, when the same value is inputted, a set of the output values is always identical. For example, it is possible to use a function F by which a certain number r ($0 \leqq r \leqq 99$) is put in correspondence with a set of all numbers r' ($0 \leqq r' \leqq 9999$) for which the residue with respect to N=100 is equal to r. In order to apply this function F to the above described embodiment, it suffices to set r=K3, and r'=K3'.

As a concrete example, in a case of r=38, the outputs of the multi-value function will be a set F(38)={38, 138, . . . , 9938}. It suffices for the user terminal **5** to transmits just one of these outputs to the key center **1**, so that it actually suffices to generate a random number R ($0 \leqq R \leqq 99$), and calculate r'=100R+r in this case. For instance, if R=22, r'=2238=(100×22)+38 will be transmitted.

At the key center **1** side, it suffices to carry out the mod **100** calculation for the received r', and the comparison with r already received earlier, to see if r=r'. If r'=2238 is actually received, r'=2238=38 (mod **100**), so that in comparison with r=38 already received earlier, it can be confirmed that r=r' indeed.

It is to be noted that the above described embodiment can be modified in the following manners.

Namely, it is possible to realize modified embodiments by changing the data to be used as an enciphering key or by changing the data to be enciphered.

In particular, after the key center **1** and the user terminal **5** shared the same key information, it becomes possible to carry out the communication by using the secret key enciphering scheme in which the enciphering key and the deciphering key are the same, so that at the step of transmitting the AP key distribution signal in FIG. **6**, in enciphering the AP key K1 and transmitting it from the key center **1** to the user terminal **5**, K3'+K4 used as an enciphering key for enciphering the AP key K1 can be replaced by K3' alone, K4 alone, or K3 alone. For instance, as shown in FIG. **8**, the AP key distribution signal can be obtained by enciphering the AP key K1 by using K3' alone as an enciphering key, instead of K3'+K4 used in FIG. **6**. Similarly, the embodiment using K4 alone or K3 alone can also be realized in obvious manners.

On the other hand, in order to confirm that the program operating on the user terminal **5** is a program from which an access is expected at the key center **1** side, it is also possible to use means other than the multi-value function. For example, the confirmation at the key center **1** side can be done by embedding some secret character string in the terminal program in advance, and returning that secret character string from the user terminal **5** to the key center **1**. In this case, the multi-value function output K3' used in FIG. **6** is obviously unnecessary, so that as shown in FIG. **9**, the random number K3 can be used instead of the multi-value function output K3' in the terminal response signal and the AP key distribution signal.

In addition, it is also possible to realize modified embodiments by changing a combination of the public key enciphering scheme E and the secret key enciphering scheme E' used in enciphering the signals between the key center **1** and the user terminal **5**.

For example, in a case the enciphering and/or deciphering speed is faster for the secret key enciphering scheme E' than for the public key enciphering scheme E, as shown in FIG. **10**, it is possible to replace the use of the public key enciphering scheme E utilized in obtaining the enciphered terminal response signal E(K3'+K4, K2*e*) in FIG. **6** by a secret key enciphering scheme E' using the random number K4 as a key to obtain the enciphered terminal response signal E'(K3'+K4, K4), such that the public key enciphering scheme E is used for enciphering the first AP key request signal from the user terminal **5** to the key center **1** alone, and the secret key enciphering scheme E' is used for enciphering all the other signals. In this case, it is unnecessary to supply the public key K2*e* to the enciphering device **63** on the user terminal **5** side, while it is necessary to supply the random

number K4 generated at the key center 1 to the deciphering device 23 instead of the secret key K2*d* on the key center 1 side, as indicated in FIG. 10.

Next, an exemplary software sales system utilizing the cipher key distribution method of the present invention as described in the above embodiment will be described.

In this software sales system, a software to be sold is enciphered and stored in a CD-ROM. Then, a user who purchased this CD-ROM installs this CD-ROM into his own user terminal and selects the desired software. After the selection, the user calls up the key center from the user terminal through a modem device, and receives the key for deciphering the selected software in exchange to the payment of the fee, such that the desired software can be deciphered and used thereafter.

This software sales system has an overall configuration as shown in FIG. 11, in which a user terminal 44 and a key center 45 are connected with each other through a public network. Also, a CD-ROM manufacturer terminal 42 and the key center 45 are connected with each other through a public network or LAN. A chargeable information is provided from an information provider 41 to the CD-ROM manufacturer terminal 42, and the CD-ROM manufacturer then manufactures a CD-ROM 43 in which this chargeable information is enciphered and stored at the CD-ROM manufacturer terminal 42, and distributes it in the market.

The CD-ROM manufacturer terminal 42 has a schematic configuration as shown In FIG. 12, which comprises an enciphering device 47 and a CD-ROM manufacturing device 48. The enciphering device 47 enciphers all the softwares of the chargeable information received from the information provider (IP) 41 one by one, by using a different AP key K1 for each software. At this point, a unique identification number ID is assigned to each software. The key center 45 manages an information indicating correspondences between the identification numbers assigned to the softwares and the AP keys used in enciphering the softwares. The CD-ROM manufacturing device 48 manufactures the CD-ROM 43 by storing the enciphered softwares outputted from the enciphering device 47, a public key K2*e* provided from the key center 45, and a sales guidance program to be activated by the user in order to select the desired software, altogether in one CD-ROM.

Now, a procedure for manufacturing the CD-ROM will be described in further detail.

When the information provider (IP) 41 hands over the softwares to be sold to the CD-ROM manufacturer, this CD-ROM manufacturer assigns a unique ID to each software received from the information provider 41.

Then, each software is separately enciphered by using an AP key K1 in correspondence to the ID of each software, and stored in the CD-ROM 43. (Note that all the AP keys are represented by the same symbol K1 here for the same of simplicity, although there are as many different AP keys as a number of softwares to be enciphered.) At the same time, the CD-ROM manufacturer also produces a correspondence table between the IDs of the softwares and the AP keys used in enciphering these softwares. Then, the manufactured CD-ROM 43 is distributed in the market, while the correspondence table is sent to the key center 45.

Now, a procedure for purchasing the software stored in the distributed CD-ROM 43 will be described in further detail.

The user at his own user terminal 44 purchases the CD-ROM 43 manufactured as described above, and installs it into a CD-ROM system of the user terminal 44. Then, the user activates the sales guidance program stored on the CD-ROM 43,and selects the desired software. (Internally, the ID of the desired software is selected at this point.)

When the desired software is selected, the user terminal 44 is connected with the key center 1 through the public network. Then, the user terminal 44 obtains the AP key K1 from the key center 45 according to the cipher key distribution method of the above embodiment, and reads out and deciphers the enciphered software at the CD-ROM system. Here, in this example, the ID of the software selected by the user is enciphered along with the random number K3 by using the public key K2*e* at the enciphering device 61 of the user terminal as shown in FIG. 4, and the resulting AP key request signal is transmitted to the key center 45. At the key center 45, using the ID of the requested software obtained by deciphering the received AP key request signal, the corresponding AP key K1 is retrieved from the AP key database 14 of the key center as shown in FIG. 5, and the retrieved AP key K1 is given to the user terminal 44 by the procedure of FIG. 6 for example, while charging the appropriate fee to this user.

As described, according to the present invention, the random numbers are generated at both of the user terminal and the key center, so that the signals between the key center and the user terminal can be changed in each access, and it is possible to check whether the user terminal is a fake one or not by enciphering the random number generated at the key center and making the user terminal to return this random number by correctly deciphering it. In addition, by inputting the random number into the multi-value function at the user terminal side, it is possible to prevent the signal between the key center and the user terminal from being identified even when the random number generation source is identified, so that it becomes impossible to draw up a block diagram of the terminal program function in order to analyze the processing content of the terminal program.

Consequently, in distributing the cipher key from the key center to the user terminal, the cipher key can be protected against the tapping of the intermediate communication line by a malicious terminal user, while it is difficult to extract any significant hint for analysis of the terminal program from the tapping result, so as to realize a protection against the falsification of the terminal program, and therefore it becomes possible to realize a safe cipher key distribution and an effective prevention of the illegitimate use and the illegitimate charging by means of the production of the dummy key center or user terminal.

It is to be noted here that, besides those already mentioned above, many modifications and variations of the above embodiments may be made without departing from the novel and advantageous features of the present invention. Accordingly, all such modifications and variations are intended to be included within the scope of the appended claims.

What is claimed is:

1. A method of cipher key distribution in a system formed by a key center having a cipher key to be distributed and a plurality of user terminals connected with the key center through a public network, the method comprising the steps of:

(a) transmitting a key request signal containing a first random number generated at each user terminal, from each user terminal to the key center, so as to indicate the cipher key required at each user terminal to the key center;

(b) transmitting a terminal check signal containing a second random number generated at the key center, from the key center to each user terminal;

(c) transmitting a terminal response signal containing the second random number and a value based on the first random number obtained according to the first random number generated at each user terminal and the second random number contained in the terminal check signal, from each user terminal to the key center;

(d) checking the second random number and the value based on the first random number contained in the terminal response signal at the key center, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and

(e) transmitting a key distribution signal containing the cipher key requested by the key request signal, from the key center to each user terminal, only when the legitimacy of the access from each user terminal is confirmed at the step (d).

2. The method of claim 1, wherein at the step (a), the key request signal is produced at each user terminal by enciphering the first random number by using a public key, and the key center obtains the first random number by deciphering the key request signal by using a secret key corresponding to the public key.

3. The method of claim 1, wherein at the step (b), the terminal check signal is produced at the key center by enciphering the second random number by using the first random number contained in the key request signal, and each user terminal obtains the second random number by deciphering the terminal check signal by using the first random number generated at each user terminal.

4. The method of claim 1, wherein at the step (c), the terminal response signal is produced at each user terminal by enciphering the second random number contained in the terminal check signal and the value based on the first random number by using a public key, and the key center obtains the second random number and the value based on the first random number contained in the terminal response signal by deciphering the terminal response signal by using a secret key corresponding to the public key.

5. The method of claim 1, wherein at the step (c), the value based on the first random number is a multi-value function output obtained at each user terminal by inputting the first random number into a multi-value function and selecting one of multiple outputs of the multi-value function.

6. The method of claim 5, wherein at the step (d), the value based on the first random number is checked at the key center by inputting the first random number contained in the key request signal into the multi-value function and comparing the value based on the first random number contained in the terminal response signal with the multiple outputs of the multi-value function.

7. The method of claim 1, wherein at the step (c), the value based on the first random number is the first random number itself.

8. The method of claim 1, wherein at the step (e), the key distribution signal is produced at the key center by enciphering the cipher key by using the second random number and the value based on the first random number contained in the terminal response signal, and each user terminal obtains the cipher key by deciphering the key distribution signal by using the second random number contained in the terminal check signal and the value based on the first random number obtained at each user terminal.

9. The method of claim 1, wherein at the step (e), the key distribution signal is produced at the key center by enciphering the cipher key by using any one of the first random number contained in the key request signal, the second random number generated at the key center, and the value based on the first random number contained in the terminal response signal, and each user terminal obtains the cipher key by deciphering the key distribution signal by using any one of the first random number generated at each user terminal, the second random number contained in the terminal check signal, and the value based on the first random number obtained at each user terminal.

10. The method of claim 1, wherein the steps (a), (b), (c), (d), and (e) include the steps of:

(a1) generating the first random number and enciphering the first random number by using a public key to produce the key request signal at each user terminal;

(a2) transmitting the key request signal produced at the step (a1) from each user terminal to the key center;

(a3) obtaining the first random number at the key center by deciphering the key request signal transmitted at the step (a2) by using a secret key corresponding to the public key;

(b1) generating the second random number and enciphering the second random number by using the first random number obtained at the step (a3) to produce the terminal check signal at the key center;

(b2) transmitting the terminal check signal produced at the step (b1) from the key center to each user terminal;

(b3) obtaining the second random number at each user terminal by deciphering the terminal check signal transmitted at the step (b2);

(c1) obtaining a multi-value function output by inputting the first random number into a multi-value function and selecting one of multiple outputs of the multi-value function at each user terminal;

(c2) enciphering the second random number obtained at the step (b3) and the multi-value function output obtained at the step (c1) by using the public key to produce the terminal response signal at each user terminal;

(c3) transmitting the terminal response signal produced at the step (c2) from each user terminal to the key center;

(c4) obtaining the second random number and the multi-value function output contained in the terminal response signal at the key center by deciphering the terminal response signal transmitted at the step (c3) by using the secret key;

(d1) checking whether the second random number obtained at the step (c4) coincides with the second random number generated at the step (b1) at the key center;

(d2) checking whether the multi-value function output obtained at the step (c4) is a true output of the multi-value function at the key center by inputting the first random number obtained at the step (a3) into the multi-value function and comparing the multi-value function output obtained at the step (c4) with the multiple outputs of the multi-value function; (d3) confirming the legitimacy of the access from each user terminal at the key center when the step (d1) confirms that the second random number deciphered at the step (c4) coincides with the second random number generated at the step (b1) and the step (d2) confirms that the multi-value function output deciphered at the step (c4) is the true output of the multi-value function;

(e1) enciphering the cipher key by using the second random number and the multi-value function output

obtained at the step (c4) to produce the key distribution signal at the key center;

(e2) transmitting the key distribution signal produced at the step (e1) from the key center to each user terminal; and

(e3) obtaining the cipher key at each user terminal by deciphering the key distribution signal transmitted at the step (e2) by using the second random number obtained at the step (b3) and the multi-value function output obtained at the step (c1).

11. A cipher key distribution system, comprising:

a key center having a cipher key to be distributed;

a plurality of user terminals connected with the key center through a public network;

key request means, provided in each user terminal, for transmitting a key request signal containing a first random number generated at each user terminal, from each user terminal to the key center, so as to indicate the cipher key required at each user terminal to the key center;

terminal check means, provided in the key center, for transmitting a terminal check signal containing a second random number generated at the key center, from the key center to each user terminal;

terminal response means, provided in each user terminal, for transmitting a terminal response signal containing the second random number and a value based on the first random number obtained according to the first random number generated at each user terminal and the second random number contained in the terminal check signal, from each user terminal to the key center;

check means, provided in the key center, for checking the second random number and the value based on the first random number contained in the terminal response signal, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and

key distribution means, provided in the key center, for transmitting a key distribution signal containing the cipher key requested by the key request signal, from the key center to each user terminal, only when the legitimacy of the access from each user terminal is confirmed by the check means.

12. The system of claim 11, wherein the key request means produces the key request signal by enciphering the first random number by using a public key, and the key center obtains the first random number by deciphering the key request signal by using a secret key corresponding to the public key.

13. The system of claim 11, wherein the terminal check means produces the terminal check signal by enciphering the second random number by using the first random number contained in the key request signal, and each user terminal obtains the second random number by deciphering the terminal check signal by using the first random number generated at each user terminal.

14. The system of claim 11, wherein the terminal response means produces the terminal response signal by enciphering the second random number contained in the terminal check signal and the value based on the first random number by using a public key, and the key center obtains the second random number and the value based on the first random number contained in the terminal response signal by deciphering the terminal response signal by using a secret key corresponding to the public key.

15. The system of claim 11, wherein the terminal response means obtains a multi-value function output as the value based on the first random number by inputting the first random number into a multi-value function and selecting one of multiple outputs of the multi-value function.

16. The system of claim 15, wherein the check means checks the value based on the first random number by inputting the first random number contained in the key request signal into the multi-value function and comparing the value based on the first random number contained in the terminal response signal with the multiple outputs of the multi-value function.

17. The system of claim 11, wherein the terminal response means uses the first random number itself as the value based on the first random number.

18. The system of claim 11, wherein the key distribution means produces the key distribution signal by enciphering the cipher key by using the second random number generated at the key center and the value based on the first random number contained in the terminal response signal, and each user terminal obtains the cipher key by deciphering the key distribution signal by using the second random number contained in the terminal check signal and the value based on the first random number obtained at each user terminal.

19. The system of claim 11, wherein the key distribution means produces the key distribution signal by enciphering the cipher key by using any one of the first random number contained in the key request signal, the second random number generated at the key center, and the value based on the first random number contained in the terminal response signal, and each user terminal obtains the cipher key by deciphering the key distribution signal by using any one of the first random number generated at each user terminal, the second random number contained in the terminal check signal, and the value based on the first random number obtained at each user terminal.

20. A cipher key distribution system, comprising:

a key center having a cipher key to be distributed; and

a plurality of user terminals connected with the key center through a public network;

wherein each user terminal includes:

means for transmitting a key request signal to the key center, receiving a terminal check signal from the key center in response to the key request signal, transmitting a terminal response signal to the key center in response to the terminal check signal, and receiving a key distribution signal from the key center in response to the terminal response signal;

means for generating a first random number;

means for producing the key request signal containing the first random number, for indicating the cipher key required at each user terminal;

means for obtaining a second random number from the terminal check signal received from the key center;

means for obtaining a value based on the first random number;

means for producing the terminal response signal containing the second random number contained in the terminal check signal and the value based on the first random number; and

means for obtaining the cipher key from the key distribution signal received from the key center; and

wherein the key center includes:

means for receiving the key request signal from each user terminal, transmitting the terminal check signal to each user terminal in response to the key request signal, receiving the terminal response signal from

each user terminal in response to the terminal check signal, and transmitting the key distribution signal to each user terminal in response to the terminal response signal;

means for obtaining the first random number from the key request signal received from each user terminal;

means for generating the second random number;

means for producing the terminal check signal containing the second random number;

means for obtaining the value based on the first random number and the second random number from the terminal response signal received from each user terminal;

means for checking the second random number and the value based on the first random number contained in the terminal response signal, according to the second random number generated at the key center and the first random number contained in the key request signal, so as to confirm a legitimacy of an access from each user terminal; and

means for producing the key distribution signal containing the cipher key requested by the key request signal, only when the legitimacy of the access from each user terminal is confirmed by said means for checking.

* * * * *

United States Patent [19]

Mollier

[11] **Patent Number: 4,683,553**

[45] **Date of Patent: Jul. 28, 1987**

[54] **METHOD AND DEVICE FOR PROTECTING SOFTWARE DELIVERED TO A USER BY A SUPPLIER**

[75] Inventor: **Jean Mollier**, Bougival, France

[73] Assignee: **Cii Honeywell Bull (Societe Anonyme)**, Paris, France

[21] Appl. No.: **828,080**

[22] Filed: **Feb. 5, 1986**

Related U.S. Application Data

[63] Continuation of Ser. No. 698,261, Feb. 5, 1985, abandoned, which is a continuation of Ser. No. 476,494, Mar. 18, 1983, abandoned.

[30] **Foreign Application Priority Data**

Mar. 18, 1982 [FR] France 82 04612

[51] **Int. Cl.**[4] **H04L 9/00**

[52] **U.S. Cl.** **380/4**; 235/382; 235/376; 364/900; 380/25

[58] **Field of Search** ... 364/200 MS File, 900 MS File; 235/376, 380, 382, 382.5, 384, 385, 487; 178/22.08, 22.09

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,105,156	8/1978	Dethloff	235/441
4,120,030	10/1978	Johnstone	364/200
4,168,396	9/1979	Best	364/900
4,211,919	7/1980	Ugon	235/487
4,278,837	7/1981	Best	364/900
4,281,216	7/1981	Hogg et al.	178/22.08
4,288,659	9/1981	Atalla	178/22.09
4,306,289	12/1981	Lumley	364/200
4,319,079	3/1982	Best	178/22.09
4,433,207	2/1984	Best	178/22.09
4,453,074	6/1984	Weinstein	235/380
4,458,315	7/1984	Uchenick	364/200
4,465,901	8/1984	Best	364/200
4,471,163	9/1984	Donald et al.	364/200
4,558,175	12/1985	Genest et al.	178/22.08

OTHER PUBLICATIONS

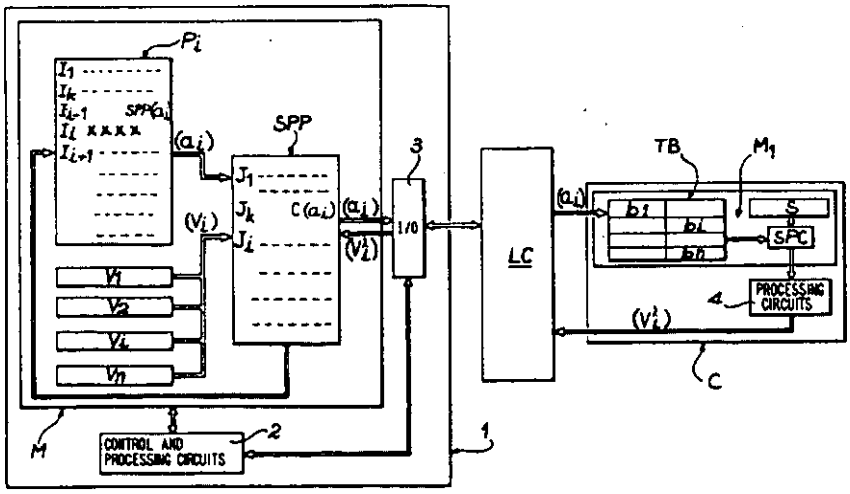
IBM Technical Disclosure Bulletin, "Protection of Memories on a Word Basis", J. Evans et al.

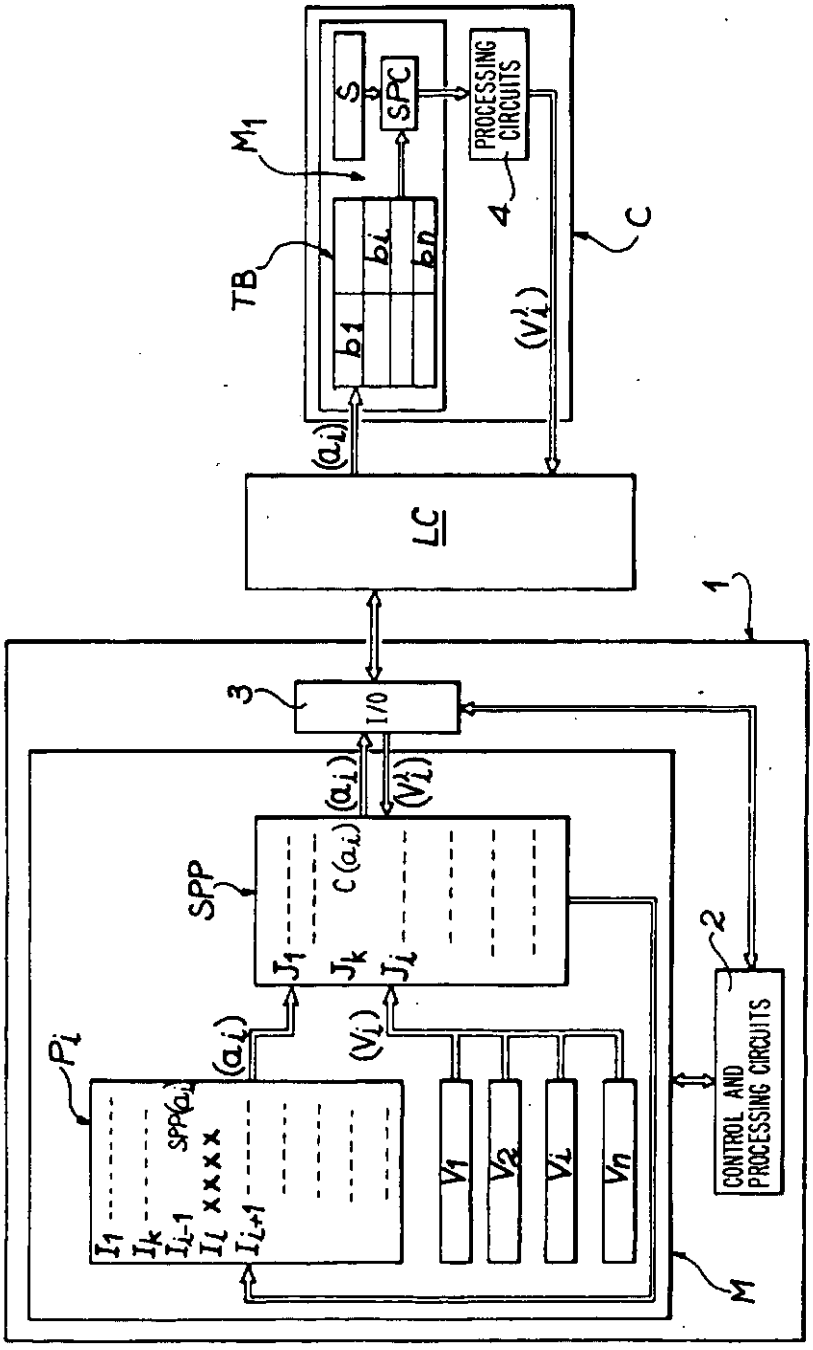
Primary Examiner—Gareth D. Shaw
Assistant Examiner—Kevin A. Kriess
Attorney, Agent, or Firm—Kerkam, Stowell, Kondracki & Clarke

[57] **ABSTRACT**

The invention relates to a method and a device for protecting software delivered to a user by a supplier. The method amounts to rendering the programs non-executable in the state in which they have been delivered to the users. With each program (P_i) there is associated a validation key defined via a main validation key (V_i) delivered by the supplier and recorded in a storage area (M) of the user's machine (1), and via a supplementary key (V'_i) computed on the lever of a card (C) issued to the user via a secret code (S) and via arguments (b_i) that identify each program (P_i) and are recorded in a storage area (M1) of the card (C).

8 Claims, 1 Drawing Figure




M1
S
SPC
PROCESSING CIRCUITS
4
C
TB
bi
bn
b1
(Vi')
(ai)
LC
1
3
I/O
(ai)
(Vi')
SPP
C(ai)
J1
Jk
Ji
2
Pi
(ai)
(Vi)
I1
Ik
Ii-1
Ii
Ii+1
SPP(ai)
xxxx
V1
V2
Vi
Vn
CONTROL AND PROCESSING CIRCUITS
M

METHOD AND DEVICE FOR PROTECTING SOFTWARE DELIVERED TO A USER BY A SUPPLIER

This is a continuation of application Ser. No. 698,261, filed Feb. 5, 1985, (now abandoned) which in turn is a continuation of Ser. No. 476,494, filed Mar. 18, 1983 (now abandoned).

BACKGROUND OF THE INVENTION

Field of the Invention

The invention relates generally to a method and a device for protecting software and is more particularly aimed at providing a method and a device by means of which a supplier who delivers software to a user remains in control of this software by rendering it non-executable in the form in which it is delivered, the execution of said software being under the control of a validation key delivered to the user by the software supplier.

Definitions

At the outset, the expressions "software", "software protection" and "non-executable software" will be defined.

1. Software and software protection

Software is understood to be at least one program in the conventional sense and, more generally, a set of programs. Generally, the organization of a software system associated with a data processing machine is such that a minimum of protection is given to the programs as a result of procedures made available by the operating system of the machine. Thus, the user program and system programs benefit from a mutual protection, each program having an assigned memory space which cannot be accessed by the other programs. As a matter of fact, such protection is inherent in the satisfactory management and smooth operation of a computer center.

The software protection provided by the invention is located at a different level. More specifically, the point in question is to give the software supplier a maximum guarantee as to the diffusion of this software. In other words and within the spirit of the invention, it is not a question of giving the software a protection in the sense of a literary and artistic property by seeking to protect the very content of the software, but it is a question of giving the owner of a software protection with respect to a potential user by giving him the means of ensuring that only this user will be able to use said software.

Indeed, from the moment a suppler negotiates with a potential user the rental or sale of a program, this supplier heretofore has not had any means of checking as to the use of this program by said user. Because of that, this user has heretofore very easily been able to take the place of the supplier to deliver, in his turn, the program to another user.

2. Non-executable software

Generally, any program is not directly executable by a data processing machine. Indeed, a program must undergo several transformations prior to its execution. Within the spirit of the invention, the program, even after undergoing the aforesaid transformations, will still remain non-executable.

Still within the spirit of the invention, this notion of non-execution of a program is not to be associated with a notion of secret. As a matter of fact, it is not a question of prohibiting the knowledge of the program to the user, but to control the use of this program by this user.

According to the invention, the supplier is thus induced to give to any potential user an incomplete or scrambled program and at least one validation key that will enable him to execute the program.

SUMMARY OF THE INVENTION

Therefore, the invention proposes a method of protecting software consisting of programs, the owner or supplier of these programs being induced to negotiate these programs with potential users who have at least one data processing machine on which these programs can be executed. So as to enable the supplier to remain in control of the diffusion of these programs once they have been issued to the users the invention comprises the steps of:

rendering non-executable the programs in the state in which they have been delivered to the users;

issuing to each user at least one portable carrier such as a card comprising at least processing circuits and a storage area where a secret code known only to the supplier and peculiar to each user has been recorded; and

for each user, associating with each program a key of predetermined validation defined in accordance with the program and with the secret code contained in the user's card, for the necessary transformation of said program into an executable program once the card is coupled or connected to the user's machine.

According to another feature of the method of the invention, the aforesaid validation key is defined, on the one hand, via a main validation key issued by the supplier and available on the user's machine and, on the other hand, via a supplementary key of computed validation on the level of the card issued to the user, via the secret code and via arguments of identification that are peculiar to each program and which have been recorded in the storage area of the card.

According to another important feature of the invention, the method comprises the steps of keeping the same arguments for the same program regardless of the user of this program; and giving a main validation key which is different, on the one hand, for each program delivered to a user and, on the other hand, for the same program delivered to another user.

The interest of such a method resides especially in the invoicing by a supplier of the software sold or rented to a user. In other words, a supplier can possess a library of n programs which can be sold or rented to a user who, through payment, will enter into possession of all or part of said library.

Thus, the supplier will define a validation key for each program chosen by a user and will issue a card which is unique to said user and in which a secret code has been recorded known solely to the supplier and unique to the user. By means of this validation key and the secret code, as described earlier, each program can be rendered executable. It will be understood, of course, that once a program has been rendered executable, it can be stored in the primary storage memory of the machine and can be reused directly without again calling upon the protection procedure according to the invention, but this procedure will again be used each time the program is reloaded in the primary storage.

BRIEF DESCRIPTION OF THE DRAWINGS

Other features, advantages and details will be more readily understood by reference to the explanatory description given hereinbelow in conjunction with the accompanying schematic drawing given by way of example and which illustrates schematically the principle of the method according to the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Let it be assumed that a person has a library of programs ($P_1 \ldots P_i \ldots P_n$). This person, who may be a supplier, is likely to rent or sell these programs to potential users who have at least one data processing machine on which these programs can be executed.

Before explaining in detail the method of the invention, which henceforth will enable this supplier to check the diffusion of the programs delivered to users, the physical means which are indispensable for the execution of the method and the nature of the data processed thereby will be described briefly.

Now, referring to the drawing, a data processing machine (1) of a potential user of the programs ($P_1 \ldots P_i \ldots P_n$) comprises at least one memory (M), circuits (2) for controlling and processing the data stored in the memory (M), and an input/output device (3).

The memory (M) is designed to contain:

at least one program (P_i) of the library of programs ($P_1 \ldots P_i \ldots P_n$) for the purpose of executing it by the machine (1);

a master main subprogram (SPP) issued by the supplier, and

main validation keys ($V_1 \ldots V_i \ldots V_n$) at the rate of one key per program. These predetermined keys are issued by the supplier and are designed to be associated with supplementary validation keys ($V'_1, \ldots V'_i, \ldots V'_n$) as will be explained hereinbelow.

The control and processing circuits (2) are conventional with specificities peculiar to the type of machine employed.

In addition to this data processing machine (1), a potential user must possess the following auxiliary equipment:

at least one portable carrier such as a card (C) issued by the supplier and designed to cooperate with the machine (1); and

a card reader (LC) coupled to the machine (1) by means of the aforsesaid input/output device (3).

The card (C) which is specific to a given user comprises as least:

one memory (M1) in which are recorded: a secret code (S);

a computer subprogram (SPC); and a table (TB) containing a set of arguments ($b_1, \ldots b_i, \ldots b_m$) to identify the programs ($P_1, \ldots P_i, \ldots P_n$); and processing circuits (4) which enable the computer subprogram (SPC) to be executed.

The reader (LC) is essentially designed to ensure the transfer of the data between the machine (1) and the card (C). The circuits making up said reader are conventional and do not have any special features, i.e. the card reader is a conventional prior art device.

In accordance with the invention, the execution of each program ($P_1 \ldots P_i \ldots P_n$) is under the supervision of a validation key which is unique to the program and to the user. Thus, each program is under the supervision of a validation key which, in actual fact, consists, with respect to the machine (1), of a main predetermined-validation key (V) and, with respect to the card (C), of a supplementary validation key (V') computed before the execution of the program.

The supplementary validation key (V') is computed by the processing circuits (4) of the card (C) which execute the computer subprogram (SPC). This subprogram (SPC) takes into account the secret code (S) recorded in the memory (M1) of the card (C) and at least one identification argument (b_i) peculiar to each program (P_i) and determined by the supplier.

A card (C) is issued to the user and all the identification arguments ($b_1 \ldots b_i \ldots b_n$) of the programs ($P_1 \ldots P_i \ldots P_n$) are prerecorded in the table (TB) stored in the memory (M1) of the card (C). Each identification argument (b_i) is, for example, an alphanumerical data item, and each program can be identified by one or more arguments. It is important to note that the identification arguments of the programs are preferably identical for all the potential users of the programs.

The addressing of the identification argument(s) ($b_1 \ldots b_i \ldots b_m$) of a program ($P_i$) for computing the supplementary validation key (V') is effected by means of identification parameters ($a_1 \ldots a_i \ldots a_m$) contained in each program and transmitted to the card (C) prior to the execution of the program.

In order to limit the storage area occupied by the table (TB) in the memory (M1) of the card, it is advantageous to identify each program by at least two identification arguments. In this way, it is not necessary to store as many identification arguments as there are programs. By way of example, if the table (TB) contains m arguments (bi) with $m \leqq n$ (n being the number of programs) and if each program is identified by two arguments, it is possible to address C^m_n programs.

The main validation key (V) on the side of the machine (1) is given by the supplier who, knowing the secret code (S) of the card (C) issued to the user and the identification arguments ($b_1 \ldots b_i \ldots b_m$) of each program ($P_1 \ldots P_i \ldots P_n$), can known in advance the value of the supplementary validation key (V') and can thus determine the value of the associated main validation key (V), said two keys (V) and (V') being combined by the subprogram (SPP) in order to render the associated program executable.

The manner in which the program is rendered non-executable is not unique and the chosen solution does not modify the principle of the invention from the moment when the execution of the program is supervised by a validation key with two levels (V, V'), such as defined above. Each program ($P_1 \ldots P_i \ldots P_n$) can be rendered non-executable or scrambled total partially.

To explain the method of the invention, let us assume a user who desires to acquire the program (P_i) of the library of programs ($P_1 \ldots P_i \ldots P_n$), each of said programs being rendered non-executable in the state in which it has been delivered.

The supplier will issue to this user:

a program tape or disk containing the set of programs ($P_1 \ldots P_i \ldots P_n$);

a card (C) such as defined above and containing in particular a secret code (S) unique to this user;

the aforesaid subprogram (SPP) which will be recorded in the memory (M) of the user's machine (1), and

the main validation key (V_i) peculiar to the program (P_i) and which will likewise be recorded in the memory (M) of the machine (1) or contained in the program (P_i).

When the user desires to execute the program (P_i), he loads, first of all, this program (P_i) in the memory (M) of his machine (1) by means of the program disk given by the supplier. Thereupon, the operating system of the machine (1) subjects this program (P_i) to the conventional transformations which are inherent in putting this program (P_1) in a state of execution. In accordance with the invention, even after undergoing these transformations, the program (P_i) is always non-executable.

To render it executable, the user will introduce the card (C) associated with his machine (1) into the reader (LC) which is coupled to the machine (1).

Let it be assumed that the program (P_i) is only scrambled in part. Referring to the drawing, let us assume that the program (P_i) contains a scrambled instruction, to wit, the instruction code for the instruction (I_i). In these conditions, the previous instructions (I_1) to (I_k) will be executed normally and the instruction (I_i-1) which precedes the instruction (I_i) will reroute to the subprogram (SPP), supplying at least one identification parameter (a_i) of the program (P_i).

The master or main subprogram (SPP) is executed and at the level of its instruction (J_k) ensures an alternate routing to the card (C) by means of the input/output device (3) under the supervision of the control circuits (2) of the machine (1). The subprogram (SPP) sends to the card (C) the identification parameter (a_i) in order to address at least one identification argument (b_i) of the table (TB) recorded in the memory (M1) of the card (C). At the level of the card (C) the computer subprogram (SPC) which takes into account the argument (b_i) of the program (P_i) and the secret code (S) of the card for the computation of the supplementary validation key (V'_i) by means of the processing circuits (4) of the card (C) is then executed.

Once the supplementary validation key (V'_i) of the program (P_i) has been calculated, the value of the said key (V'_i) is sent back by means of the reader (LC) and the input/output (3) circuit of the machine (1) to the main subprogram (SPP). The instruction (J_i) of the subprogram (SPP) will take this supplementary validation key (V'_i) into account as well as the main validation key (V_i) which has been prerecorded in the memory (M) of the machine (1) and is associated with the program (P_i). By means of these two validation keys (V_i, V'_i), the main subprogram (SPP) will unscramble the instruction (I_i) for the program (P_i). By way of example, the two keys (V_i) and (V'_i) can be binary configurations with p bits with the subprogram (SPP) which executes a logic operation such as "EXCLUSIVE OR" upon these two binary configurations, the result of this logic operation giving the instruction code of the instruction (I_i) for the program (P_i). In this way, the instruction (I_i) for the program (P_i) is unscrambled and the program (P_i) can then be executed in its entirety.

According to another feature of the invention, the same user can possess a single card (C) for several machines (1). In this case, the same program cannot be applied simultaneously to several machines, because the user's card must remain coupled to one machine in order to ensure the execution of the program on said machine.

Needless to say that a user can purchase the same program several times, say, twice. He will then have to have two different cards in order to apply the same program simultaneously to two machines.

Finally, if one card is issued for the possible execution of m programs among n available programs and if the user desires to obtain the execution of other programs that have not been purchased initially, it is not necessary for the supplier to issue another card to him. It suffices that the supplier simply supply the main validation key of the new program(s) without having to modify the card that has already been issued.

To enable the supplier of the programs to remain in control of their diffusion, it is important that the data recorded on the level of each card cannot be accessed from the outside in order to avoid any fraud.

While the invention has been described in connection with a particular embodiment, this description is not intended to be by way of limitation and resort should be made to the appended claims which define the full scope of the invention.

I claim:

1. A system for protecting software programs (P_1, . . . , P_i, . . . P_n) adapted to be executed on a data processing machine (1) of a user of the software programs, said machine having at least one memory (M), control and processing circuits (2), and an input/output device (3), the system comprising:

a card (C), specific to the user, possessing at least one memory (M1) and processing circuits (4), and

a card reader (LC) coupled with the input/output device (3) of the machine (1) and with the card (C) to enable data transfer therebetween; the memory (M) of the machine (1) containing at least one program (P_i) delivered by a supplier of the software programs, the one program including an identification parameter (a_i) which identifies the one program and having a scrambled portion which renders the one program non-executable on the machine, containing a main validation key code (V_i), specific to the one program, issued by the supplier, and containing a master program (SPP); the memory (M1) of the card (C) containing at least one secret code (S) specific to the user and known only to the suppler, and identification arguments which identify the programs, at least one of said identification arguments (b_i) identifying said one program, the card having means responsive to the identification parameter (a_i) contained in the one program (P_i) for addressing said identification argument (b_i), and the processing circuits (4) of the card having means for computing a supplementary validation key code (V'_i) from the secret code (S) and the addressed identification argument (b_i) of the program (P_i) and for transferring the supplementary validation key code to the machine; and wherein the master program (SPP) is formed to combine the supplementary validation key code (V'_i) and the main validation key code (V_i) for unscrambling the scrambled portion of the program (P_i) and rendering the program executable.

2. A method of protecting software programs (P_1, . . . P_i, . . . P_n) delivered by a supplier to prospective users, each user possessing a data processing machine (1) on which said programs can be executed, the method comprising:

prior to delivery to a user rendering the programs nonexecutable in the state in which the programs are delivered, said rendering comprising scrambling a portion of each program (P_i) such that a predetermined validation key (V_i, V'_i) is required for unscrambling the program (P_i) to transform it into an executable state, said predetermined validation key comprising a combination of a main vali-

dation key (V_i) and a supplementary validation key (V'_i), the main validation key being defined in accordance with the program (P_i) and a secret code (S) which is unique to the user and known solely to the supplier, and the program (P_i) having an identification parameter (a_i) which identifies the program;

coupling to the user's machine a portable card having processing circuits (4) and a storage area (M_1) in which are recorded the user's unique secret code and identification arguments ($b_1, \ldots b_i, \ldots b_n$) which are associated with the identification parameters ($a_1, \ldots a_i, \ldots a_n$) of the programs ($P_1, \ldots P_i, \ldots P_n$);

storing in a memory (M) of the user's machine the program (P_i) and the corresponding main validation code (V_i);

transferring to the card the identification parameter (a_i);

producing in the processing circuits of the card the supplementary validation key (V'_i) for the program (P_i) as a function of the secret code and an associated identification argument (b_i) and supplying said supplementary validation key to the user's machine;

combining in the user's machine, the main validation key and the supplementary validation key to produce the predetermined validation key; and

applying the predetermined validation key to the program (P_i) to unscramble the program (P_i) and transform it into an executable state.

3. The method as defined in claim 2 further comprising:

prerecording in each user's card prior to delivery of the card to the user identical identification arguments (b_i) for identifying the same program regardless of the user of said program, and

wherein said storing comprises storing in each user's machine a main validation key (V_i) which differs for each program (P_i) delivered to the user and which differs from the main validation key for the same program (P_i) delivered to another user.

4. The method as defined in claim 3, wherein said prerecording further includes:

prerecording in the storage area of the card the identification arguments ($b_1, \ldots b_i, \ldots b_n$) of the programs in the form of a table (TB); and wherein the card is formed to permit addressing of at least one said identification argument (b_i) of the program (P_i) by means of at least one associated identification parameter (a_i) which is transferred to the card by the user's machine.

5. The method as defined in claim 2 comprising:

recording in the memory of the user's machine a main subprogram (SPP);

said subprogram (SPP) being formed to transfer the identification parameters (a_i) to the card (C), for addressing said identification arguments (b_i), to receive from the processing circuits (4) of the card (C) the supplementary validation key (V'_i) produced from the arguments (b_i) addressed by the identification parameters (a_i) and from the secret code (S) of the card (C), and to combine said supplementary validation key (V'_i) with the main validation key (V_i) of the program (P_i) to be executed in order to produce said predetermined validation key and render said program executable.

6. The method as defined in claim 2, wherein said scrambling comprises rendering at least one instruction of each program non-executable through scrambling of an instruction code of the instruction.

7. The method as defined in claim 6 further comprising forming each main validation key (V_i) and each supplementary validation key (V'_i) as a binary configuration with p bits.

8. The method as defined in claim 7, wherein, for the purpose of unscrambling the instruction code, the method further comprises forming the main validation key (V_i) and the supplementary validation key (V'_i) so as to unscramble of the instruction code upon the keys being combined in a logic operation.

* * * * *